

E N C Y C L O P E D I A   O F  
**Espionage, Intelligence, and Security**



E N C Y C L O P E D I A O F  
**Espionage, Intelligence, and Security**

*This page intentionally left blank*

E N C Y C L O P E D I A O F  
Espionage, Intelligence, and Security

K. LEE LERNER AND BRENDA WILMOTH LERNER, EDITORS

v o l u m e  
1 1  
A - E







## Encyclopedia of Espionage, Intelligence, and Security

K. Lee Lerner and Brenda Wilmoth Lerner, editors

**Project Editor**  
Stephen Cusack

**Editorial**  
Erin Bealmear, Joann Cerrito, Jim Craddock,  
Miranda Ferrara, Kristin Hart, Melissa Hill,  
Carol Schwartz, Christine Tomassini, Michael  
J. Tyrkus, Peter Gareffa

**Permissions**  
Lori Hines

**Imaging and Multimedia**  
Dean Dauphinais, Leitha Etheridge-Sims, Mary  
K. Grimes, Lezlie Light, Luke Rademacher

**Product Design**  
Kate Scheible

**Manufacturing**  
Rhonda Williams

© 2004 by Gale. Gale is an imprint of The  
Gale Group, Inc., a division of Thomson  
Learning, Inc.

Gale and Design™ and Thomson Learning™  
are trademarks used herein under license.

*For more information, contact*  
The Gale Group, Inc.  
27500 Drake Rd.  
Farmington Hills, MI 48331-3535  
Or you can visit our Internet site at  
<http://www.gale.com>

### ALL RIGHTS RESERVED

No part of this work covered by the copyright  
hereon may be reproduced or used in  
any form or by any means—graphic,  
electronic, or mechanical, including  
photocopying, recording, taping, Web  
distribution, or information storage retrieval  
systems—without the written permission of  
the publisher.

For permission to use material from this  
product, submit your request via Web at  
<http://www.gale-edit.com/permissions>, or you  
may download our Permissions Request form  
and submit your request by fax or mail to:

*Permissions Department*  
The Gale Group, Inc.  
27500 Drake Rd.  
Farmington Hills, MI 48331-3535  
Permissions Hotline:  
248-699-8006 or 800-877-4253, ext. 8006  
Fax: 248-699-8074 or 800-762-4058

### Cover Photos

Volume 1: Ethel and Julius Rosenberg  
following arraignment on charges of  
espionage, August 23, 1950.  
©Bettmann/Corbis

Volume 2: SR-71 Blackbird, c. 1991. ©Corbis

Volume 3: Clean-up crews scour the American  
Media Inc. building in Boca Raton, Florida,  
after the discovery of anthrax spores, October  
9, 2001. AP/Wide World Photos.

While every effort has been made to  
ensure the reliability of the information  
presented in this publication, The Gale Group,  
Inc. does not guarantee the accuracy of  
the data contained herein. The Gale Group,  
Inc. accepts no payment for listing; and  
inclusion in the publication of any  
organization, agency, institution, publication,  
service, or individual does not imply  
endorsement of the editors or publisher.  
Errors brought to the attention of the  
publisher and verified to the satisfaction of  
the publisher will be corrected in future  
editions.

### Library of Congress Cataloging-in-Publication Data

Encyclopedia of espionage, intelligence, and security / K. Lee Lerner  
and Brenda Wilmoth Lerner, editors.  
p. cm.

Includes bibliographical references and index.

ISBN 0-7876-7546-6 (set : hardcover : alk. paper) — ISBN  
0-7876-7686-1 (v. 1) — ISBN 0-7876-7687-X (v. 2) — ISBN 0-7876-7688-8  
(v. 3)

1. Espionage—Encyclopedias. 2. Intelligence service—Encyclopedias.  
3. Security systems—Encyclopedias. I. Lerner, K. Lee. II. Lerner,  
Brenda Wilmoth.  
JF1525.I6E63 2004  
327.12'03—dc21

2003011097

This title is available as an e-book.  
ISBN 0-7876-7762-0

Contact your Gale sales representative for ordering information.

Printed in the United States of America  
10 9 8 7 6 5 4 3 2 1

# Contents

INTRODUCTION	VII
ADVISORS AND CONTRIBUTORS	XI
LIST OF ENTRIES	XIII
 The Encyclopedia of Espionage, Intelligence, and Security	 1
 GLOSSARY	 289
 CHRONOLOGY	 317
 SOURCES	 353
 INDEX	 403

*This page intentionally left blank*

# Introduction

In composing *The Encyclopedia of Espionage, Intelligence, and Security (EEIS)*, our goal was to shape a modern encyclopedia offering immediate value to our intended readers by emphasizing matters of espionage, intelligence, and security most frequently in the news.

*EEIS* is not intended as a classical “spy book,” filled with tales of daring operations. Instead, within a framework of historical overviews, *EEIS* emphasizes the scientific foundations, applications of technology, and organizational structure of modern espionage, intelligence, and security. High school and early undergraduate students can use this book to expand upon their developing awareness of the fundamentals of science, mathematics, and government as they begin the serious study of contemporary issues.

*EEIS* is also intended to serve more advanced readers as a valuable quick reference and as a foundation for advanced study of current events.

*EEIS* devotes an extensive number of articles to agencies and strategies involved in emerging concepts of homeland security in the United States. Faced with a daunting amount of information provided by agencies, organizations, and institutes seeking to put their best foot forward, we have attempted to allocate space to the topics comprising *EEIS* based upon their relevance to some unique facet of espionage, intelligence, or security—especially with regard to science and technology issues—as opposed to awarding space related to power of the agency or availability of material.

A fundamental understanding of science allows citizens to discern hype and disregard hysteria, especially with regard to privacy issues. Spy satellites powerful enough to read the details of license plates do so at peril of missing events a few steps away. With regard to electronic intercepts, the capability to identify what to carefully examine—often a decision driven by mathematical analysis—has become as essential as the capacity to gather the intelligence itself. Somewhere between the scrutiny of

Big Brother and the deliberately blind eye lie the shadows into which terrorists often slip.

With an emphasis on the realistic possibilities and limitations of science, we hope that *EEIS* finds a useful and unique place on the reference shelf.

It seems inevitable that within the first half of the twenty-first century, biological weapons may eclipse nuclear and chemical weapons in terms of potential threats to civilization. Because informed and reasoned public policy debates on issues of biological warfare and bioterrorism can only take place when there is a fundamental understanding of the science underpinning competing arguments, *EEIS* places special emphasis on the multifaceted influence and applications of the biological sciences and emerging biometric technologies. Future generations of effective intelligence and law enforcement officers seeking to thwart the threats posed by tyrants, terrorists, and the technologies of mass destruction might be required to be as knowledgeable in the terminology of epidemiology as they are with the tradecraft of espionage.

Knowledge is power. In a time where news can overwhelm and in fact, too easily mingle with opinion, it is our hope that *EEIS* will provide readers with greater insight to measure vulnerability and risks, and correspondingly, an increased ability to make informed judgments concerning the potential benefits and costs of espionage, intelligence, and security matters.

■ K. LEE LERNER & BRENDA WILMOTH LERNER, EDITORS  
CORNWALL, U.K.  
MAY, 2003

## How to Use the Book

*The Encyclopedia of Espionage, Intelligence, and Security* was not intended to contain a compendium of weapons systems. Although *EEIS* carries brief overviews of specifically selected systems commonly used in modern intelligence operations, readers interested in detailed information regarding weapons systems are recommended

to *Jane's Strategic Weapon Systems*, or *Jane's Defense Equipment Library*.

Although *EEIS* contains overview of significant historical periods and events, for those readers interested in additional information regarding the history of espionage operations and biographies of intelligence personnel, the editors recommend Jeffrey T. Richelson's *A Century of Spies: Intelligence in the Twentieth Century* (Oxford University Press, 1995), Vincent Buranelli and Nan Buranelli's *Spy/Counterspy: An Encyclopedia of Espionage* (New York: McGraw-Hill, 1982), and Allen Dulles', *The Craft of Intelligence* (New York: Harper & Row, 1963).

The articles in *EEIS* are meant to be understandable by anyone with a curiosity about topics in espionage, intelligence, and security matters, and this first edition of the book has been designed with ready reference in mind:

- Entries are arranged alphabetically. In an effort to facilitate easy use of this encyclopedia, and to attempt order in a chaotic universe of names and acronyms the editors have adopted a "common use" approach. Where an agency, organization, or program is known best by its acronym, the entry related to that organization will be listed by the acronym (e.g. FEMA is used instead of Federal Emergency Management Agency). To facilitate use, the editors have included a number of "jumps" or cross-referenced titles that will guide readers to desired entries.
- To avoid a log jam of terms starting with "Federal" and "United States," titles were broken to most accurately reflect the content emphasized or subject of agency authority.
- "**See Also**" references at the end of entries alert the readers to related entries not specifically mentioned in the body of the text that may provide additional or interesting resource material.
- An extensive **Glossary** of terms and acronyms is included to help the reader navigate the technical information found in *EEIS*.
- The **Chronology** includes significant events related to the content of the encyclopedia. Often accompanied by brief explanations, the most current entries date represent events that occurred just as *EEIS* went to press.
- A **Sources** section lists the most worthwhile print material and web sites we encountered in the compilation of this volume. It is there for the inspired reader who wants more information on the people and discoveries covered in this volume.
- A comprehensive general **Index** guides the reader to topics and persons mentioned in the book. Bolded page references refer the reader to the term's full entry.
- The editors and authors have attempted to explain scientific concepts clearly and simply, without sacrificing fundamental accuracy. Accordingly, an advanced understanding of physics, chemistry, or biochemistry is not assumed or required. Students and other readers should not, for example, be intimidated or deterred by the complex names of biochemical molecules—where necessary for complete understanding, sufficient information regarding scientific terms is provided.
- To the greatest extent possible we have attempted to use Arabic names instead of their Latinized versions. Where required for clarity we have included Latinized names in parentheses after the Arabic version. Alas, we could not retain some diacritical marks (e.g. bars over vowels, dots under consonants). Because there is no generally accepted rule or consensus regarding the format of translated Arabic names, we have adopted the straightforward, and we hope sensitive, policy of using names as they are used or cited in their region of origin.
- *EEIS* relies on open source material and no classified or potentially dangerous information is included. Articles have been specifically edited to remove potential "how to" information. All articles have been prepared and reviewed by experts who were tasked with ensuring accuracy, appropriateness, and accessibility of language.
- With regard to entries regarding terrorist organizations, *EEIS* faced a serious dilemma. For obvious reasons, it was difficult to obtain balanced, impartial, and independently verifiable information regarding these organizations, nor could *EEIS* swell to incorporate lengthy scholarly analysis and counter-analysis of these organizations without losing focus on science and technology issues. As a compromise intended to serve students and readers seeking initial reference materials related to organizations often in the news, *EEIS* incorporates a series of supplemental articles to convey the information contained in the U.S. Department of State annual report to Congress titled, *Patterns of Global Terrorism, 2001*. These articles contain the language, assertions of fact, and views of the U.S. Department of State. Readers are encouraged to seek additional information from current U.S. Department of State resources and independent non-governmental scholarly publications that deal with the myriad of issues surrounding the nature and activities of alleged terrorist organizations. A number of governmental and non-governmental publications that deal with these issues are cited in the bibliographic sources section located near the index.

Key *EEIS* articles are signed by their authors. Brief entries were compiled by experienced researchers and reviewed by experts. In the spirit of numerous independent scientific watchdog groups, during the preparation of *EEIS* no contributors held a declared affiliation with any intelligence or security organization. This editorial policy not only allowed a positive vetting of contributors, but also assured an independence of perspective and an emphasis on the fundamentals of science as opposed to unconfirmable "insider" information.

When the only verifiable or attributable source of information for an entry comes from documents or information provided by a governmental organization (e.g., the U.S. Department of State), the editors endeavored to carefully note when the language used and perspective offered was that of the governmental organization.

Although some research contributors requested anonymity, no pseudonyms are used herein.

## Acknowledgments

The editors wish to thank Herbert Romerstein, former USIA Soviet Disinformation Officer and Coordinator of Programs to Counter Soviet Active Measures, United States Information Agency, for his assistance in compiling selected articles.

The editors wish to thank Lee Wilmoth Lerner for his assistance in compiling technical engineering data for inclusion in *EEIS*.

The editors acknowledge the assistance of the members of the Federation of American Scientists for the provision of reports and materials used in the preparation of selected articles.

Although certainly not on the scale of the challenge to provide security for a nation with approximately 85 deep-draft ports, 600,000 bridges, 55,000 independent water treatment systems, 100 nuclear power plants, and countless miles of tunnels, pipelines, and electrical and communications infrastructure, the task of incorporating changes brought on by creation of the Department of Homeland Security—and the most massive reorganization of the United States government since World War II—as this book went to press provided a unique challenge to *EEIS*

writers and advisors. The editors appreciate their dedication and willingness to scrap copy, roll up their sleeves, and tackle anew the smorgasbord of name and terminology changes.

As publishing deadlines loomed, *EEIS* was also well served by a research staff dedicated to incorporating the latest relevant events—especially information related to the search for weapons of mass destruction—that took place during war in Iraq in March and April of 2003.

*EEIS* advisors, researchers, and writers tenaciously attempted to incorporate the most current information available as *EEIS* went to press. The editors pass any credit or marks for success in that effort, and reserve for themselves full responsibility for omissions.

The editors gratefully acknowledge the assistance of many at St. James Press for their help in preparing *The Encyclopedia of Espionage, Intelligence, and Security*. The editors extend thanks to Mr. Peter Gareffa and Ms. Meggin Condino for their faith in this project. Most directly, the editors wish to acknowledge and thank the project editor, Mr. Stephen Cusack, for his talented oversight and for his tireless quest for secure engaging pictures for *EEIS*.

The editors lovingly dedicate this book to the memory of Wallace Schaffer, Jr., HM3, USNR, who died on January 8, 1968, in Thua Thien (Hue) Province, Vietnam.

“A small rock holds back a great wave.”—Homer, *The Odyssey*.

*This page intentionally left blank*

## Advisors and Contributors

**Julie Berwald, Ph.D.**

*Geophysicist, writer on marine science, environmental biology, and issues in geophysics.*  
Austin, Texas

**Robert G. Best, Ph.D.**

*Clinical cytogeneticist and medical geneticist who has written on a range of bioscience issues*  
Director, Division of Genetics  
University of South Carolina School of Medicine

**Tim Borden, Ph.D.**

*Doctorate in History from Indiana University, and is an inspector with the U.S. Bureau of Customs and Border Protection*  
Toledo, Ohio

**Brian Cobb, Ph.D.**

*Bioscience writer, researcher*  
Institute for Molecular and Human Genetics  
Georgetown University, Washington, D.C.

**Cecilia Colomé, Ph.D.**

*Astrophysicist, translator, and science writer*  
Austin, Texas

**Laurie Duncan, Ph.D.**

*Geologist, science writer, and researcher*  
Austin, Texas

**William J. Engle, P.E.**

*Writer on contemporary geophysics issues and the impacts of science and technology on history*  
Exxon-Mobil Oil Corporation (Rt.) New Orleans, Louisiana

**Antonio Farina, M.D., Ph.D.**

*Physician, researcher, and writer on medical science issues*  
Assistant Professor, University of Bologna, Italy

**Christopher T. Fisher, Ph.D.**

*Assistant Professor, Department of African American Studies and the Department of History*  
The College of New Jersey, Ewing, New Jersey

**Larry Gilman, Ph.D.**

*Electrical engineer and science writer*  
Sharon, Vermont

**William Haneberg, Ph.D.**

*Former research scientist and professor, now an independent consulting geologist and science writer*  
Portland, Oregon

**Brian D. Hoyle, Ph.D.**

*Science writer and Chief Microbiologist, Government of New Brunswick from 1993 to 1997*  
Nova Scotia, Canada

**Joseph Patterson Hyder**

*Writer on the historical impacts of science and technology*  
University of Tennessee College of Law, Knoxville, Tennessee

**Alexandr Ioffe, Ph.D.**

*Writer on the history of science and researcher with the Geological Institute of Russian Academy of Sciences in Moscow*  
Russian Academy of Sciences, Moscow

**Judson Knight**

*Science writer, researcher, and editor*  
Knight Agency Research Services, Atlanta, Georgia

**Michael Lambert, Ph.D.**

*Researcher at the Great Plains/Rocky Mountain Hazardous Substance Research Center and at the U.S. Naval Research Laboratory*  
Manhattan, Kansas

**Adrienne Wilmoth Lerner**

*Writer of various articles on the history of science, archaeology, and the evolution of security-related law*  
University of Tennessee College of Law, Knoxville, Tennessee



**Agnes Lichanska, Ph.D.**

*Science writer who has conducted research at the Department of Medical Genetics and Ophthalmology at Queen's University of Belfast (Northern Ireland)*

University of Queensland, Brisbane, Australia

**Eric v.d. Luft, Ph.D., M.L.S.**

*Writer on cultural, scientific, and intellectual history, and philosophy*

Curator of Historical Collections  
SUNY Upstate Medical University, Syracuse, New York

**Martin Manning**

*Served on the Economic Security Team, Office of International Information Programs, U.S. Department of State*

Bureau of Public Diplomacy  
U.S. Department of State, Washington, D.C.

**Kelli Miller**

*Served as news writer and producer for Inside Science TV News at the American Institute of Physics (AIP) and as executive producer of Discoveries & Breakthroughs Inside Science*

Atlanta, Georgia

**Caryn E. Neumann**

*Instructor and doctoral candidate in the Department of History at Ohio State University*

Columbus, Ohio

**Mike O'Neal, Ph.D.**

*Independent scholar and writer*

Moscow, Idaho

**Belinda M. Rowland, Ph.D.**

*Science and medical writer*

Voorheesville, New York

**Judyth Sassoon, Ph.D., ARCS**

*Science writer with research experience in NMR and X-ray crystallography techniques*

Department of Biology & Biochemistry  
University of Bath, United Kingdom

**Morgan Simpson**

*Aerospace Engineer*

National Aeronautical and Space Administration (NASA)

Kennedy Space Center, Cape Canaveral, Florida

**Constance K. Stein, Ph.D.**

*Writer on medical and bioscience issues related to modern genetics*

Director of Cytogenetics, Assistant Director of Molecular Diagnostics

SUNY Upstate Medical University, Syracuse, New York

**Tabitha Sparks, Ph.D.**

*Marion L. Brittain fellow, Georgia Institute of Technology and Fellow, Center for Humanistic Inquiry, Emory University*

Atlanta, Georgia

**David Tulloch**

*Science and technology writer*

Wellington, New Zealand

**Michael T. Van Dyke, Ph.D.**

*Served as visiting assistant professor, Department of American Thought & Language*

Michigan State University, East Lansing, Michigan

**Stephanie Watson**

*Science writer specializing in the social impacts of science and technology*

Smyrna, Georgia

**Simon Wendt, Ph.D.**

*Ph.D. candidate in Modern History and History instructor*

John F. Kennedy Institute for North American Studies, Free University of Berlin, Germany

# List of Entries

## I A I

Abu Nidal Organization (ANO)  
Abu Sayyaf Group (ASG)  
Abwehr  
ADFGX Cipher  
Aflatoxin  
Africa, Modern U.S. Security Policy and Interventions  
Agent Orange  
Air and Water Purification, Security Issues  
Air Force Intelligence, United States  
Air Force Office of Special Investigations, United States  
Air Marshals, United States  
Air Plume and Chemical Analysis  
Aircraft Carrier  
Airline Security  
Al-Aqsa Martyrs Brigade  
Alex Boncayao Brigade (ABB)  
Al-Gama'a al-Islamiyya (Islamic Group, IG)  
Al-Ittihad al-Islami (AIAI)  
Al-Jama'a al-Islamiyyah al-Muqatilah bi-Libya  
Al-Jihad  
Allied Democratic Forces (ADF)  
Al-Qaeda (also known as Al-Qaida)  
Americas, Modern U.S. Security Policy and Interventions  
Ames (Aldrich H.) Espionage Case  
Anthrax  
Anthrax, Terrorist Use as a Biological Weapon  
Anthrax Vaccine  
Anthrax Weaponization  
Antiballistic Missile Treaty  
Antibiotics  
Anti-Imperialist Territorial Nuclei (NTA)  
APIS (Advance Passenger Information System)  
Archeology and Artifacts, Protection of during War  
Architecture and Structural Security  
Area 51 (Groom Lake, Nevada)  
Argentina, Intelligence and Security  
Argonne National Laboratory  
Armed Islamic Group (GIA)  
Arms Control, United States Bureau

Army for the Liberation of Rwanda (ALIR)  
Army Security Agency  
'Asbat al-Ansar  
Asilomar Conference  
Assassination  
Assassination Weapons, Mechanical  
Asymmetric Warfare  
ATF (United States Bureau of Alcohol, Tobacco, and Firearms)  
Atmospheric Release Advisory Capability (ARAC)  
Audio Amplifiers  
Aum Supreme Truth (Aum)  
Australia, Intelligence and Security  
Austria, Intelligence and Security  
Aviation Intelligence, History  
Aviation Security Screeners, United States

## I B I

B-2 Bomber  
B-52  
Bacterial Biology  
Ballistic Fingerprints  
Ballistic Missile Defense Organization, United States  
Ballistic Missiles  
Balloon Reconnaissance, History  
Basque Fatherland and Liberty (ETA)  
Bathymetric Maps  
Bay of Pigs  
Belgium, Intelligence and Security Agencies  
Belly Buster Hand Drill  
Berlin Airlift  
Berlin Tunnel  
Berlin Wall  
Biochemical Assassination Weapons  
Biocontainment Laboratories  
Biodetectors  
Bio-Engineered Tissue Constructs  
Bio-Flips  
Biological and Biomimetic Systems  
Biological and Toxin Weapons Convention  
Biological Input/Output Systems (BIOS)

- Biological Warfare  
 Biological Warfare, Advanced Diagnostics  
 Biological Weapons, Genetic Identification  
 Bio-Magnetics  
 Biomedical Technologies  
 Biometrics  
 Bio-Optic Synthetic Systems (BOSS)  
 Biosensor Technologies  
 BioShield Project  
 Bioterrorism  
 Bioterrorism, Protective Measures  
 Black Chamber  
 Black Ops  
 Black Tom Explosion  
 Bletchley Park  
 Bolivia, Intelligence and Security  
 Bomb Damage, Forensic Assessment  
 Bomb Detection Devices  
 Bombe  
 Bosnia and Herzegovina, Intelligence and Security  
 Botulinum Toxin  
 Brain-Machine Interfaces  
 Brain Wave Scanners  
 Brazil, Intelligence and Security  
 British Terrorism Act  
 Brookhaven National Laboratory  
 Bubonic Plague  
 Bugs (Microphones) and Bug Detectors  
 Bush Administration (1989–1993), United States  
     National Security Policy  
 Bush Administration (2001–), United States  
     National Security Policy
- I C I**
- Cambodian Freedom Fighters (CFF)  
 Cambridge University Spy Ring  
 Cameras  
 Cameras, Miniature  
 Canada, Counter-Terrorism Policy  
 Canada, Intelligence and Security  
 Canine Substance Detection  
 Carter Administration (1977–1981), United States  
     National Security Policy  
 CDC (United States Centers for Disease Control  
     and Prevention)  
 CERN  
 Chechen-Russian Conflict  
 Chemical and Biological Defense Information  
     Analysis Center (CBIAC)  
 Chemical and Biological Detection Technologies  
 Chemical Biological Incident Response Force,  
     United States  
 Chemical Safety and Hazard Investigation Board  
     (USCSB), United States  
 Chemical Safety: Emergency Responses  
 Chemical Warfare  
 Chemistry: Applications in Espionage, Intelligence,  
     and Security Issues  
 Chernobyl Nuclear Power Plant Accident, Detection  
     and Monitoring  
 Chile, Intelligence and Security  
 China, Intelligence and Security
- Chinese Espionage against the United States  
 Church Committee  
 CIA (United States Central Intelligence Agency)  
 CIA (CSI), Center for the Study of Intelligence  
 CIA Directorate of Science and Technology (DS&T)  
 CIA, Foreign Broadcast Information Service  
 CIA, Formation and History  
 CIA, Legal Restriction  
 Cipher Disk  
 Cipher Key  
 Cipher Machines  
 Cipher Pad  
 Civil Aviation Security, United States  
 Civil War, Espionage and Intelligence  
 Classified Information  
 Clinton Administration (1993–2001), United States  
     National Security Policy  
 Clipper Chip  
 Closed-Circuit Television (CCTV)  
 Coast Guard (USCG), United States  
 Coast Guard National Response Center  
 Code Name  
 Code Word  
 Codes and Ciphers  
 Codes, Fast and Scalable Scientific Computation  
 COINTELPRO  
 Cold War (1945–1950), The Start of the Atomic Age  
 Cold War (1950–1972)  
 Cold War (1972–1989): The Collapse of the Soviet  
     Union  
 Colombia, Intelligence and Security  
 Colossus I  
 COMINT (Communications Intelligence)  
 Commerce Department Intelligence and Security  
     Responsibilities, United States  
 Commission on Civil Rights, United States  
 Communicable Diseases, Isolation, and Quarantine  
 Communications System, United States National  
 Comprehensive Test Ban Treaty (CTBT)  
 Computer and Electronic Data Destruction  
 Computer Fraud and Abuse Act of 1986  
 Computer Hackers  
 Computer Hardware Security  
 Computer Keystroke Recorder  
 Computer Modeling  
 Computer Security Act (1987)  
 Computer Software Security  
 Computer Virus  
 Concealment Devices  
 Consumer Product Safety Commission (CPSC),  
     United States  
 Continuity Irish Republican Army (CIRA)  
 Continuity of Government, United States  
 Continuous Assisted Performance (CAP)  
 Coordinator for Counterterrorism, United States  
     Office  
 Copyright Security  
 Counterfeit Currency, Technology and the  
     Manufacture  
 Counter-Intelligence  
 Counter-Terrorism Rewards Program  
 Covert Operations  
 Crib  
 Crime Prevention, Intelligence Agencies

Critical Infrastructure  
 Critical Infrastructure Assurance Office (CIAO),  
 United States  
 Croatia, Intelligence and Security  
 Cruise Missile  
 Cryptology and Number Theory  
 Cryptology, History  
 Cryptonym  
 Cuba, Intelligence and Security  
 Cuban Missile Crisis  
 Customs Service, United States  
 Cyanide  
 Cyber Security  
 Cyber Security Warning Network  
 Czech Republic, Intelligence and Security

## I D I

D Notice  
 DARPA (Defense Advanced Research Projects  
 Agency)  
 Data Mining  
 DCI (Director of the Central Intelligence Agency)  
 DEA (Drug Enforcement Administration)  
 Dead Drop Spike  
 Dead-Letter Box  
 Decontamination Methods  
 Decryption  
 Defense Information Systems Agency, United  
 States  
 Defense Nuclear Facilities Safety Board, United  
 States  
 Defense Security Service, United States  
 Delta Force  
 Department of State Bureau of Intelligence and  
 Research, United States  
 Department of State, United States  
 DIA (Defense Intelligence Agency)  
 Dial Tone Decoder  
 Diplomatic Security (DS), United States Bureau  
 Dirty Tricks  
 Disinformation  
 DNA  
 DNA Fingerprinting  
 DNA Recognition Instruments  
 DNA Sequences, Unique  
 Document Destruction  
 Document Forgery  
 DOD (United States Department of Defense)  
 DOE (United States Department of Energy)  
 Domestic Emergency Support Team, United States  
 Domestic Intelligence  
 Domestic Preparedness Office (NDPO), United  
 States National  
 Doo Transmitter  
 Dosimetry  
 Double Agents  
 Drop  
 Drug Control Policy, United States Office of  
 National  
 Drug Intelligence Estimates  
 Dual Use Technology

## I E I

E-2C  
 Ebola Virus  
 E-Bomb  
 Echelon  
 Economic Espionage  
 Economic Intelligence  
 Egypt, Intelligence and Security  
 Eichmann, Adolf: Israeli Capture  
 Eisenhower Administration (1953–1961), United  
 States National Security Policy  
 El Salvador, Intelligence and Security  
 Electromagnetic Pulse  
 Electromagnetic Spectrum  
 Electromagnetic Weapons, Biochemical Effects  
 Electronic Communication Intercepts, Legal Issues  
 Electronic Countermeasures  
 Electronic Warfare  
 Electro-Optical Intelligence  
 Electrophoresis  
 EM Wave Scanners  
 Emergency Response Teams  
 Encryption of Data  
 Enduring Freedom, Operation  
 Energy Directed Weapons  
 Energy Regulatory Commission, United States  
 Federal  
 Energy Technologies  
 Engraving and Printing, United States Bureau  
 Engulf, Operation  
 Enigma  
 Entry-Exit Registration System, United States  
 National Security  
 Environmental Issues Impact on Security  
 Environmental Measurements Laboratory  
 EPA (Environmental Protection Agency)  
 Epidemiology  
 Espionage  
 Espionage Act of 1917  
 Espionage and Intelligence, Early Historical  
 Foundations  
 Estonia, Intelligence and Security  
 European Union  
 Executive Orders and Presidential Directives  
 Explosive Coal

## I F I

F-117A Stealth Fighter  
 FAA (United States Federal Aviation  
 Administration)  
 Facility Security  
 FBI (United States Federal Bureau of Investigation)  
 FCC (United States Federal Communications  
 Commission)  
 FDA (United States Food and Drug Administration)  
 Federal Protective Service, United States  
 Federal Reserve System, United States  
 FEMA (United States Federal Emergency  
 Management Agency)  
 FEST (United States Foreign Emergency Support  
 Team)

Fingerprint Analysis  
 Finland, Intelligence and Security  
 First of October Anti-fascist Resistance Group (GRAPO)  
 FISH (German *Geheimschreiber* Cipher Machine)  
 Fission  
 Flame Analysis  
 Flight Data Recorders  
 FM Transmitters  
 FOIA (Freedom of Information Act)  
 Food Supply, Counter-Terrorism  
 Ford Administration (1974–1977), United States National Security Policy  
 Foreign Assets Control (OFAC), United States Office  
 Foreign Intelligence Surveillance Act  
 Foreign Intelligence Surveillance Court of Review  
 Forensic Geology in Military or Intelligence Operations  
 Forensic Science  
 Forensic Voice and Tape Analysis  
 France, Counter-Terrorism Policy  
 France, Intelligence and Security  
 French Underground during World War II, Communication and Codes  
 Fusion

## I G I

G–2  
 GAO (General Accounting Office, United States)  
 Gas Chromatograph-Mass Spectrometer  
 General Services Administration, United States  
 Genetic Code  
 Genetic Information: Ethics, Privacy and Security Issues  
 Genetic Technology  
 Genomics  
 Geologic and Topographical Influences on Military and Intelligence Operations  
 Geospatial Imagery  
 Germany, Counter-Terrorism Policy  
 Germany, Intelligence and Security  
 Gestapo  
 GIS  
 Global Communications, United States Office  
*Glomar Explorer*  
 Government Ethics (USOGE), United States Office  
 GPS  
 Great Game  
 Greece, Intelligence and Security  
 GSM Encryption  
 Guatemala, Intelligence and Security  
 Guerilla Warfare

## I H I

HAMAS (Islamic Resistance Movement)  
 Hanssen (Robert) Espionage Case  
 Harakat ul-Jihad-I-Islami (HUJI) (Movement of Islamic Holy War)

Harakat ul-Jihad-I-Islami/Bangladesh (HUJI-B) (Movement of Islamic Holy War)  
 Harakat ul-Mujahidin (HUM) (Movement of Holy Warriors)  
 Hardening  
 Health and Human Services Department, United States  
 Heavy Water Technology  
 Hemorrhagic Fevers and Diseases  
 Hizballah (Party of God)  
 Homeland Security, United States Department of  
 HUMINT (Human Intelligence)  
 Hungary, Intelligence and Security  
 Hypersonic Aircraft

## |||

IBIS (Interagency Border Inspection System)  
 IDENT (Automated Biometric Identification System)  
 Identity Theft  
 IFF (Identification Friend or Foe)  
 IMF (International Monetary Fund)  
 IMINT (Imagery Intelligence)  
 India, Intelligence and Security  
 Indonesia, Intelligence and Security  
 Infectious Disease, Threats to Security  
 Information Security  
 Information Security (OIS), United States Office of Information Warfare  
 Infrared Detection Devices  
 Infrastructure Protection Center (NIPC), United States National  
 INS (United States Immigration and Naturalization Service)  
 INSCOM (United States Army Intelligence and Security Command)  
 INSPASS (Immigration and Naturalization Service Passenger Accelerated Service System)  
 Inspector General (OIG), Office of the Intelligence  
 Intelligence Agent  
 Intelligence and Counterespionage Careers  
 Intelligence and Democracy: Issues and Conflicts  
 Intelligence and International Law  
 Intelligence and Law Enforcement Agencies  
 Intelligence & Research (INR), United States Bureau of  
 Intelligence Authorization Acts, United States Congress  
 Intelligence Community  
 Intelligence Literature  
 Intelligence Officer  
 Intelligence Policy and Review (OIPR), United States Office of  
 Intelligence Support, United States Office of Intelligence, United States Congressional Oversight of  
 Interagency Security Committee, United States  
 Internal Revenue Service, United States  
 International Atomic Energy Agency (IAEA)  
 International Narcotics and Law Enforcement Affairs (INL), United States Bureau of

Internet  
 Internet: Dynamic and Static Addresses  
 Internet Spam and Fraud  
 Internet Spider  
 Internet Surveillance  
 Internet Tracking and Tracing  
 INTERPOL (International Criminal Police Organization)  
 Interpol, United States National Central Bureau  
 Interrogation  
 Interrogation: Torture Techniques and Technologies  
 Iran-Contra Affair  
 Iran, Intelligence and Security  
 Iranian Hostage Crisis  
 Iranian Nuclear Programs  
 Iraq, Intelligence and Security Agencies in  
 Iraq War: Prelude to War (The International Debate Over the Use and Effectiveness of Weapons Inspections)  
 Iraq War (Immediate Aftermath)  
 Iraqi Freedom, Operation (2003 War Against Iraq)  
 Ireland, Intelligence and Security  
 Irish Republican Army (IRA)  
 Islamic Army of Aden (IAA)  
 Islamic Movement of Uzbekistan (IMU)  
 Isotopic Analysis  
 Israel, Counter-Terrorism Policy  
 Israel, Intelligence and Security  
 Italy, Intelligence and Security

## I J I

Jaish-e-Mohammed (JEM) (Army of Mohammed)  
 Japan, Intelligence and Security  
 Japanese Red Army (JRA)  
 JDAM (Joint Direct Attack Munition)  
 Jemaah Islamiya (JI)  
 Johnson Administration (1963–1969), United States National Security Policy  
 Joint Chiefs of Staff, United States  
 Jordan, Intelligence and Security  
 J-STARS  
 Justice Department, United States

## I K I

Kahane Chai (Kach)  
 Kennedy Administration (1961–1963), United States National Security Policy  
 Kenya, Bombing of United States Embassy  
 KGB (*Komitet Gosudarstvennoi Bezopasnosti*, USSR Committee of State Security)  
 Khobar Towers Bombing Incident  
 Knives  
 Korean War  
 Kosovo, NATO Intervention  
 Kumpulan Mujahidin Malaysia (KMM)  
 Kurdistan Workers' Party (PKK)  
 Kuwait Oil Fires, Persian Gulf War

## I L I

Language Training and Skills  
 Laser  
 Laser Listening Devices  
 Lashkar-e-Tayyiba (LT) (Army of the Righteous)  
 Law Enforcement, Responses to Terrorism  
 Law Enforcement Training Center (FLETC), United States Federal  
 Lawrence Berkeley National Laboratory (LBL)  
 Lawrence Livermore National Laboratory (LLNL)  
 League of Nations  
 Lebanon, Bombing of U.S. Embassy and Marine Barracks  
 Less-Lethal Weapons Technology  
 L-Gel Decontamination Reagent  
 Liberation Tigers of Tamil Eelam (LTTE)  
 Libraries and Information Science (NCLIS), United States National Commission on  
 Libya, Intelligence and Security  
 Libya, U.S. Attack (1986)  
 LIDAR (Light Detection and Ranging)  
 Lock-Picking  
 Locks and Keys  
 Looking Glass  
 Lord Haw-Haw  
 Lord's Resistance Army (LRA)  
 Los Alamos National Laboratory  
 Loyalist Volunteer Force (LVF)

## I M I

Mail Sanitization  
 Malicious Data  
 Manhattan Project  
 Mapping Technology  
 Marine Mammal Program  
 McCarthyism  
 Measurement and Signatures Intelligence (MASINT)  
 Metal Detectors  
 Meteorology and Weather Alteration  
 Mexico, Intelligence and Security  
 MI5 (British Security Service)  
 MI6 (British Secret Intelligence Service)  
 Microbiology: Applications to Espionage, Intelligence, and Security  
 Microchip  
 Microfilms  
 Microphones  
 Microscopes  
 Microwave Weaponry, High Power (HPM)  
 Middle East, Modern U.S. Security Policy and Interventions  
 Military Police, United States  
 MOAB (Massive Ordnance Air Burst Bomb)  
 Molecular Biology: Applications to Espionage, Intelligence, and Security  
 Moles  
 Monroe Doctrine  
 Morocco, Intelligence and Security  
 Mossad  
 Motion Sensors

Mount Weather  
 Movies, Espionage and Intelligence Portrayals  
 Mujahedin-e Khalq Organization (MEK or MKO)  
 Mustard Gas

## I N I

NAIS (National Automated Immigration Lookout System)  
 Nanotechnology  
 Napoleonic Wars, Espionage during  
 NASA (National Air and Space Administration)  
 National Archives and Records Administration (NARA), United States  
 National Command Authority  
 National Drug Threat Assessment  
 National Information Infrastructure Protection Act, United States  
 National Intelligence Estimate  
 National Interagency Civil-Military Institute (NICI), United States  
 National Liberation Army (ELN)—Colombia  
 National Military Joint Intelligence Center  
 National Preparedness Strategy, United States  
 National Response Team, United States  
 National Security Act (1947)  
 National Security Advisor, United States  
 National Security Strategy, United States  
 National Security Telecommunications Advisory Committee  
 National Telecommunications Information Administration, and Security for the Radio Frequency Spectrum, United States  
 NATO (North Atlantic Treaty Organization)  
 Natural Resources and National Security  
 Navy Criminal Investigative Service (NCIS)  
 NCIX (National Counterintelligence Executive), United States Office of the  
 NDIC (Department of Justice National Drug Intelligence Center)  
 Near Space Environment  
 Nerve Gas  
 Netherlands, Intelligence and Security  
 New People's Army (NPA)  
 New Zealand, Intelligence and Security  
 NFIB (United States National Foreign Intelligence Board)  
 NIC (National Intelligence Council)  
 Nicaragua, Intelligence and Security  
 Nigeria, Intelligence and Security  
 Night Vision Scopes  
 NIH (National Institutes of Health)  
 NIJ (National Institute of Justice)  
 NIMA (National Imagery and Mapping Agency)  
 NIMH (National Institute of Mental Health)  
 NIST (National Institute of Standards and Technology), United States  
 NIST Computer Security Division, United States  
 Nixon Administration (1969–1974), United States National Security Policy  
 NMIC (National Maritime Intelligence Center)  
 NNSA (United States National Nuclear Security Administration)

NOAA (National Oceanic & Atmospheric Administration)  
 Noise Generators  
 Nongovernmental Global Intelligence and Security  
 Non-Proliferation and National Security, United States  
 NORAD  
 North Korea, Intelligence and Security  
 North Korean Nuclear Weapons Programs  
 Norway, Intelligence and Security  
 NRO (National Reconnaissance Office)  
 NSA (United States National Security Agency)  
 NSC (National Security Council)  
 NSC (National Security Council), History  
 NSF (National Science Foundation)  
 NTSB (National Transportation Safety Board)  
 Nuclear Detection Devices  
 Nuclear Emergency Support Team, United States  
 Nuclear Power Plants, Security  
 Nuclear Reactors  
 Nuclear Regulatory Commission (NRC), United States  
 Nuclear Spectroscopy  
 Nuclear Weapons  
 Nuclear Winter  
 Nucleic Acid Analyzer (HANAA)

## I O I

Oak Ridge National Laboratory (ORNL)  
 Official Secrets Act, United Kingdom  
 OPEC (Organization of Petroleum Exporting Countries)  
 Operation Liberty Shield  
 Operation Magic  
 Operation Mongoose  
 Operation Shamrock  
 Orange Volunteers (OV)  
 OSS (United States Office of Strategic Services)

## I P I

P-3 Orion Anti-Submarine Maritime Reconnaissance Aircraft  
 Pacific Northwest National Laboratory  
 Pakistan, Intelligence and Security  
 Palestine Islamic Jihad (PIJ)  
 Palestine Liberation Front (PLF)  
 Palestinian Authority, Intelligence and Security  
 PanAm 103, (Trial of Libyan Intelligence Agents)  
 Panama Canal  
 Parabolic Microphones  
 Pathogen Genomic Sequencing  
 Pathogen Transmission  
 Pathogens  
 Patriot Act Terrorist Exclusion List  
 Patriot Act, United States  
 Patriot Missile System  
 Pearl Harbor, Japanese Attack on  
 People Against Gangsterism and Drugs (PAGAD)  
 Persian Gulf War  
 Peru, Intelligence and Security

Petroleum Reserves, Determination  
 PFIAB (President's Foreign Intelligence Advisory Board)  
 Phoenix Program  
 Photo Alteration  
 Photographic Interpretation Center (NPIC), United States National  
 Photographic Resolution  
 Photography, High-Altitude  
 Playfair Cipher  
 Plum Island Animal Disease Center  
 Poland, Intelligence and Security  
 Politics: The Briefings of United States Presidential Candidates  
 Pollard Espionage Case  
 Polygraphs  
 Polymerase Chain Reaction (PCR)  
 Popular Front for the Liberation of Palestine (PFLP)  
 Popular Front for the Liberation of Palestine-General Command (PFLP-GC)  
 Port Security  
 PORTPASS (Port Passenger Accelerated Service System)  
 Portugal, Intelligence and Security  
 Postal Security  
 Postal Service (USPS), United States  
 Potassium Iodide  
 President of the United States (Executive Command and Control of Intelligence Agencies)  
 Pretty Good Privacy (PGP)  
 Privacy: Legal and Ethical Issues  
 Profiling  
 Propaganda, Uses and Psychology  
 Pseudoscience Intelligence Studies  
 Psychotropic Drugs  
 Public Health Service (PHS), United States  
*Pueblo* Incident  
 Purple Machine

## I Q I

Quantum Physics: Applications to Espionage, Intelligence, and Security Issues

## I R I

RADAR  
 RADAR, Synthetic Aperture  
 Radiation, Biological Damage  
 Radio Direction Finding Equipment  
 Radio Frequency (RF) Weapons  
 Radioactive Waste Storage  
 Radiological Emergency Response Plan, United States Federal  
 Reagan Administration (1981–1989), United States National Security Policy  
 Real IRA (RIRA)  
 Reconnaissance  
 Red Code  
 Red Hand Defenders (RHD)  
 Red Orchestra  
 Remote Sensing

Retina and Iris Scans  
 Revolutionary Armed Forces of Colombia (FARC)  
 Revolutionary Nuclei  
 Revolutionary Organization 17 November (17 November)  
 Revolutionary People's Liberation Party/Front (DHKP/C)  
 Revolutionary Proletarian Initiative Nuclei (NIPR)  
 Revolutionary United Front (RUF)  
 Revolutionary War, Espionage and Intelligence  
 RF Detection  
 Ricin  
 Robotic Vehicles  
 Romania, Intelligence and Security  
 Room 40  
 Rosenberg (Ethel and Julius) Espionage Case  
 Russia, Intelligence and Security  
 Russian Nuclear Materials, Security Issues

## I S I

Sabotage  
 Salafist Group for Call and Combat (GSPC)  
 Salmonella and Salmonella Food Poisoning  
 Sandia National Laboratories  
 Sarin Gas  
 Satellite Technology Exports to the People's Republic of China (PRC)  
 Satellites, Non-Governmental High Resolution  
 Satellites, Spy  
 Saudi Arabia, Intelligence and Security  
 Scanning Technologies  
 SEAL Teams  
 Secret Service, United States  
 Secret Writing  
 Security Clearance Investigations  
 Security, Infrastructure Protection, and Counterterrorism, United States National Coordinator  
 Security Policy Board, United States  
 Seismograph  
 Seismology for Monitoring Explosions  
 Senate Select Committee on Intelligence, United States  
 Sendero Luminoso (Shining Path, or SL)  
 SENTRI (Secure Electronic Network for Travelers' Rapid Inspection)  
 September 11 Terrorist Attacks on the United States  
 Sequencing  
 Serbia, Intelligence and Security  
 Sex-for-Secrets Scandal  
 Ships Designed for Intelligence Collection  
 "Shoe Bomber"  
 Shoe Transmitter  
 Short-Wave Transmitters  
 SIGINT (Signals Intelligence)  
 Silencers  
 Skunk Works  
 Slovakia, Intelligence and Security  
 Slovenia, Intelligence and Security  
 Smallpox  
 Smallpox Vaccine



SOE (Special Operations Executive)  
 Soldier and Biological Chemical Command  
 (SBCCOM), United States Army  
 Solid-Phase Microextraction Techniques  
 Soman  
 SONAR  
 SOSUS (Sound Surveillance System)  
 South Africa, Intelligence and Security  
 South Korea, Intelligence and Security  
 Soviet Union (USSR), Intelligence and Security  
 Space Shuttle  
 Spain, Intelligence and Security  
 Spanish-American War  
 Special Collection Service, United States  
 Special Counsel and Security Related  
 “Whistleblower” Protection Issues, United States  
 Office  
 Special Operations Command, United States  
 Special Relationship: Technology Sharing between  
 the Intelligence Agencies of the United States  
 and United Kingdom  
 Spectroscopy  
 Spores  
 SR-71 Blackbird  
 START I Treaty  
 START II  
 STASI  
 Stealth Technology  
 Steganography  
 Strategic Defense Initiative and National Missile  
 Defense  
 Strategic Petroleum Reserve, United States  
 Sudan, Intelligence and Security  
 Suez Canal  
 Supercomputers  
 Surgeon General and Nuclear, Biological, and  
 Chemical Defense, United States Office  
 Sweden, Intelligence and Security  
 Switzerland, Intelligence and Security  
 Syria, Intelligence and Security

## III

Tabun  
 Taiwan, Intelligence and Security  
 Taser  
 Technical Intelligence  
 Technology Transfer Center (NTTC), Emergency  
 Response Technology Program  
 Telemetry  
 Telephone Caller Identification (Caller ID)  
 Telephone Recording Laws  
 Telephone Recording System  
 Telephone Scrambler  
 Telephone Tap Detector  
 Terror Alert System, United States  
 Terrorism, Domestic (United States)  
 Terrorism, Intelligence Based Threat and Risk  
 Assessments  
 Terrorism, Philosophical and Ideological Origins  
 Terrorism Risk Insurance  
 Terrorist and Para-State Organizations  
 Terrorist Organization List, United States

Terrorist Organizations, Freezing of Assets  
 Terrorist Threat Integration Center  
 Thin Layer Chromatography  
 TIA (Terrorism Information Awareness)  
 Tissue-Based Biosensors  
 Tokyo Rose  
 Toxicology  
 Toxins  
 Tradecraft  
 Transportation Department, United States  
 Treasury Department, United States  
 Truman Administration (1945–1953), United States  
 National Security Policy  
 Truth Serum  
 Tularemia  
 Tunisian Combatant Group (TCG)  
 Tupac Amaru Revolutionary Movement (MRTA)  
 Turkey, Intelligence and Security  
 Turkish Hizballah  
 Typex

## III

U-2 Incident  
 U-2 Spy Plane  
 Ukraine, Intelligence and Security  
 Ulster Defense Association/Ulster Freedom Fighters  
 (UDA/UVF)  
 Ultra, Operation  
 Underground Facilities, Geologic and Structural  
 Considerations in the Construction  
 Undersea Espionage: Nuclear vs. Fast Attack Subs  
 Unexploded Ordnance and Mines  
 United Kingdom, Counter-Terrorism Policy  
 United Kingdom, Intelligence and Security  
 United Nations Security Council  
 United Self-Defense Forces/Group of Colombia  
 (*AUC Autodefensas Unidas de Colombia*)  
 United States, Counter-Terrorism Policy  
 United States, Intelligence and Security  
 United States Intelligence, History  
 Unmanned Aerial Vehicles (UAVs)  
 Uranium  
 Uranium Depletion Weapons  
 USAMRICD (United States Army Medical Research  
 Institute of Chemical Defense)  
 USAMRIID (United States Army Medical Research  
 Institute of Infectious Diseases)  
 USS *Cole*  
 USS *Liberty*  
 USSTRATCOM (United States Strategic Command)

## III

Vaccination  
 Vaccines  
 Variola Virus  
 Venezuela, Intelligence and Security  
 Venona  
 Vietnam War  
 Viral Biology

Viral Exposure Therapy, Antiviral Drug  
Development  
Voice Alteration, Electronic  
Voice of America (VOA), United States  
Vozrozhdeniye Island, Soviet and Russian  
Biochemical Facility  
Vulnerability Assessments  
VX Agent

## I W I

Walker Family Spy Ring  
War of 1812  
Water Supply: Counter-Terrorism  
Watergate  
Weapon-Grade Plutonium and Uranium, Tracking  
Weapons of Mass Destruction

Weapons of Mass Destruction, Detection  
Windtalkers  
World Health Organization (WHO)  
World Trade Center, 1993 Terrorist Attack  
World Trade Center, 2001 Terrorist Attack  
World War I  
World War I: Loss of the German Codebook  
World War II  
World War II: Allied Invasion of Sicily and “The  
Man Who Never Was”  
World War II, The Surrender of the Italian Army  
World War II, United States Breaking of Japanese  
Naval Codes

## I Z I

Zoonoses

*This page intentionally left blank*



## Abu Nidal Organization (ANO)

Abu Nidal Organization (ANO) is identified by the United States Department of State as an international terrorist organization led by Sabri al-Banna. Split from the Palestine Liberation Army (PLO) in 1974, the ANO is comprised of various functional committees, including political, military, and financial committees.

The Abu Nidal Organization (ANO) also operates as, or is known as; Fatah Revolutionary Council, Arab Revolutionary Brigades, Black September, and Revolutionary Organization of Socialist Muslims.

**Organization activities.** The ANO has carried out terrorist attacks in 20 countries, killing or injuring almost 900 persons. Targets have included the United States, the United Kingdom, France, Israel, moderate Palestinians, the PLO, and various Arab countries. Major attacks included the Rome and Vienna airports in December 1985, the Neve Shalom synagogue in Istanbul, and the Pan Am Flight 73 hijacking in Karachi in September 1986, along with the City of Poros day-excursion ship attack in Greece in July, 1988. The ANO is suspected of assassinating PLO deputy chief Abu Iyad and PLO security chief Abu Hul in Tunis in January, 1991. ANO assassinated a Jordanian diplomat in Lebanon in January, 1994, and has been linked to the killing of the PLO representative there. As of May 2002, the ANO has not attacked Western targets since the late 1980s. ANO leader Abu Nidal was found dead in Baghdad, Iraq in August 2002. Following Nidal's death and subsequent disruption of ANO by Operation Iraqi Freedom in 2003, the fate of the organization remained uncertain.

Membership in the ANO is estimated at a few hundred plus a limited overseas support structure. Al-Banna relocated to Iraq in December 1998, where the group maintains a presence. ANO has had an operational presence in Lebanon including in several Palestinian refugee

camps. Financial problems and internal disorganization have reduced the group's activities and capabilities. Authorities shut down the ANO's operations in Libya and Egypt in 1999. The ANO has demonstrated ability to operate over wide areas, including the Middle East, Asia, and Europe. They have also received considerable support, including safe haven, training, logistic assistance, and financial aid from Iraq, Libya, and Syria (until 1987), in addition to close support for selected operations.

### ■ FURTHER READING :

#### ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001, Annual Report: On the record briefing. May 21, 2002 <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

#### SEE ALSO

*Terrorism, Philosophical and Ideological Origins Terrorist and Para-State Organizations Terrorist Organization List, United States Terrorist Organizations, Freezing of Assets*

## Abu Sayyaf Group (ASG)

The Abu Sayyaf Group (ASG) is the most violent of the Islamic separatist groups operating in the southern Philippines. Some ASG leaders have studied or worked in the Middle East and reportedly fought in Afghanistan during the Soviet war. The group split from the Moro National Liberation Front in the early 1990s under the leadership of

Abdurajak Abubakar Janjalani, who was killed in a clash with Philippine police on 18 December, 1998. His younger brother, Khadaffy Janjalani, has replaced him as the nominal leader of the group, which is composed of several semi-autonomous factions.

**Organization activities.** The ASG engages in kidnappings for ransom, bombings, assassinations, and extortion. Although from time to time it claims that its motivation is to promote an independent Islamic state in western Mindanao and the Sulu Archipelago, areas in the southern Philippines heavily populated by Muslims, the ASG now appears to use terror mainly for financial profit. The group's first large-scale action was a raid on the town of Ipil in Mindanao in April 1995. In April of 2000, an ASG faction kidnapped 21 persons, including 10 foreign tourists, from a resort in Malaysia. Separately in 2000, the group abducted several foreign journalists, three Malaysians, and a United States citizen. On 27 May 2001, the ASG kidnapped three U.S. citizens and 17 Filipinos from a tourist resort in Palawan, Philippines. Several of the hostages, including one U.S. citizen, were murdered.

A few hundred ASG fighters make up the core group, but at least 1000 individuals motivated by the prospect of receiving ransom payments for foreign hostages allegedly joined the group in 2000–2001.

The ASG was founded in Basilan Province, and mainly operates there and in the neighboring provinces of Sulu and Tawi-Tawi in the Sulu Archipelago. It also operates in the Zamboanga peninsula, and members occasionally travel to Manila and other parts of the country. The group expanded its operations to Malaysia in 2000 when it abducted foreigners from a tourist resort.

The ASG is largely self-financed through ransom and extortion, but they may also receive support from Islamic extremists in the Middle East and South Asia. Libya publicly paid millions of dollars for the release of the foreign hostages seized from Malaysia in 2000.

## ■ FURTHER READING :

### ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001, Annual Report: On the record briefing. May 21, 2002 <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

### SEE ALSO

*Terrorism, Philosophical and Ideological Origins*  
*Terrorist and Para-State Organizations*  
*Terrorist Organization List, United States*  
*Terrorist Organizations, Freezing of Assets*

## Abwehr

■ ADRIENNE WILMOTH LERNER

The Abwehr was the German military intelligence organization from 1866 to 1944. The organization predates the emergence of Germany itself, and was founded to gather intelligence information for the Prussian government during a war with neighboring Austria. After initial successes, the organization was expanded during the Franco-Prussian War in 1870. Under the direction of Wilhelm Stieber, Abwehr located, infiltrated, and reported on French defensive positions and operations. The Prussians claimed victory, largely because of the success of Abwehr agents. In 1871, Prussia united with other independent German states to form the nation of Germany. The new country adopted much of the former Prussian government and military structure, including the Abwehr.

The intelligence agency was again tested at the outbreak of World War I in 1914. German agents worked to pinpoint the location and strength of the Allied forces, helping the German forces to invade and progress through northern France before stalemated trench warfare began. New military technology changed the nature of espionage. Agency director Walther Nicolai recognized the need for a modernized intelligence force and reorganized the department to include experts in wire tapping, munitions manufacturing, shipping, and encryption. The agency tapped enemy communications wires, intercepting and deciphering Allied dispatches with measured accomplishment. The Abwehr sent several agents to spy on the manufacture of poison gas in France, and tracked munitions production and shipping in Britain. The organization sent saboteurs to disrupt the shipment of arms from America to Allied forces in Europe. Several ships were sunk in transit after being identified by agents as smuggling arms. German agents, often acting on information collected by Abwehr, set fire to several American weapons factories and storage facilities. While the Abwehr was generally successful, the loss of the German codebook to British intelligence somewhat undermined the agency's ultimate efficacy during the war.

After World War I, the Abwehr ceased operation under the terms of the Versailles Treaty. The intelligence service was re-established in 1921. When the Nazis gained control of Germany in the 1930s, some members of the intelligence agency began to spy on their own government. The Nazis created a separate intelligence organization, the *Sicherheitsdienst*, or Security Service, headed by Reinhard Heydrich. In 1935, the new Abwehr director, Wilhelm Canaris, and Heydrich reached an agreement about the roles of each agency, but both trained and maintained their own espionage forces. Canaris reorganized the Abwehr into three branches: espionage, counter-espionage, and saboteurs. He appointed three distinguished Abwehr agents to lead the branches, but only on condition that they were not members of the Nazi party.

This aroused the suspicion of rival Security Service. The two agencies came into conflict on several occasions, and as Heydrich gained power, he persuaded the government to investigate members of the Abwehr for espionage and treason. Several members of the Abwehr were arrested in 1939. Though a handful of the agency's highest ranking officials were active as double-agents or as members of the Resistance, the organization as a whole continued its espionage operations on behalf of the German government.

At the outbreak of World War II, Abwehr resumed operations similar to those carried out during World War I. The agency was in charge of tracking troops and munitions transports, tapping wires and intercepting radio messages, and infiltrating foreign intelligence and military units. Abwehr placed two operatives inside the British intelligence agency for two years, and developed a highly successful encryption device called the Enigma machine. Agents tracked and monitored various resistance movements in occupied Europe, and even sabotaged military and government strongholds behind Allied lines.

Canaris made the United States one of Abwehr's primary targets even before America's entry into the conflict. By 1942, German agents were operating from within all of America's top armaments manufacturers. Abwehr scored perhaps its greatest victories in the area of industrial espionage, as agents managed to steal the blueprint for every major American airplane produced for the war effort.

One of the Abwehr's responsibilities during World War II was the extraction of information from prisoners of war. While Abwehr agents remained largely in control of seeking strategic information from British, French, and American prisoners, the Nazi government issued a special directive to various branches of the military regarding Russian prisoners of war. The Commissar Order, as it became known, instructed the Army to handle Russian prisoners as harshly as they deemed necessary for the retrieval of military information. At one time, German concentration camps held more than 1.5 million Russian prisoners. Canaris himself raised several objections to this policy, largely on the grounds that it undermined the authority and efficacy of his agency and could cripple the German war effort.

In 1944, Heinrich Himmler, head of the Gestapo, the Nazi secret police, assumed control of Abwehr after an unsuccessful assassination attempt on Adolf Hitler and several other high ranking Nazi officials. Himmler suspected that the plot was the work of agents inside the government, most especially the Abwehr. The July Plot also exposed the work of those Abwehr agents who had intentionally leaked sensitive information to the Allies. Several agents, including Canaris, were charged with treason and executed. The Abwehr was then dissolved.

#### SEE ALSO

*Bletchley Park*  
*Cipher Machines*

*Germany, Intelligence and Security*  
*World War I: Loss of the German Codebook*

## Accelerated Strategic Computing Initiative (ASCI).

SEE *Lawrence Livermore National Laboratory (LLNL)*.

## Achille Lauro.

SEE *Palestine Liberation Front (PLF)*.

## Acoustic Bullets.

SEE *Audio Amplifiers*.

---

# ADFGX Cipher

---

■ JUDSON KNIGHT

The ADFGX cipher, sometimes referred to as the ADFGVX cipher, is one of the most famous codes in the entire history of cryptography. Introduced by the Germans in World War I, it is based on an ancient idea of associating letters with positions on a grid. Variations on the code have made communication possible across the walls of prison cells, and further intricacies added through the technique of transposition have made the code unbreakable without the aid of a computer.

Greek historian Polybius (fl.c. 200 B.C.) introduced what became known as the Polybius square, a 5 x 5 grid that used the 24 letters of the Greek alphabet. Each letter had a unique position identifiable by a coordinate system that numbered the rows and columns. For example, *A* was one column to the right of the point of origin, and one row down, so its coordinate would be 11. In the English alphabet, two letters are combined in a single square so that the 26 letters fit into the 25-square grid. Supposing *I* and *J* are combined, then *K* would be at position 25—two rows down, and five squares over.

Over the centuries that followed, the Polybius square made possible a system of taps or knocks whereby prisoners could pass messages to one another across walls. Applied by groups ranging from Russian anarchists to American prisoners of war in Vietnam, the system has been described by writers as diverse as Arthur Koestler in *Darkness at Noon*, Aleksandr Solzhenitsyn in *The Gulag*

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i/j	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

A polybius cipher square showing a grid that assigns a code number to each letter of the alphabet. In this square, for example, the letter M would be coded as number 32.

*Archipelago*, and Senator John S. McCain in *Faith of Our Fathers*. It has undergone countless variations based on the needs of the users—for example, a 6 x 6 grid for the 33 letters of the Russian alphabet—but the basic principle remains the same. According to the English-language grid described earlier, for instance, *K* would be rendered by two rapid knocks or taps, a short break, and then five rapid knocks or taps.

**The ADFGX Cipher in World War I.** The ADFGX cipher, developed by German army radio officer Fritz Nebel (1891–1967), made its appearance on March 5, 1918, when the Germans used it in a wireless transmission on the western front. Instead of the numerals 1 through 5 along a side of the Polybius square, Nebel’s cipher applied the letters *A*, *D*, *F*, *G*, and *X*, which he chose because their equivalents in Morse code were so dissimilar that confusion was unlikely. (For example, *A* is one dot and two dashes, while *D* is one dash and two dots.) Three months later, on June 1, the German army added the letter *V* to make a sixth row and column. The 6 x 6 grid of the ADFGVX cipher allowed the inclusion of the 10 numerals from 0 to 9, like its predecessor.

The brilliance of the ADFGX cipher lay in the fact that, unlike ordinary codes, the frequency of letters such as *E* was not easy to recognize. Furthermore, the code could become even more challenging by applying a system of transposition. Suppose a message is written out in ADFGVX format—that is, as a series of two-letter combinations

using just those six letters. That string of letters is then placed in a matrix under the letters of a chosen keyword, such as *KAISER*, which an army in wartime would typically change every day. Then the letters of the keyword are placed in alphabetical order—in this case, spelling *AEIKRS*, with the corresponding columns moved as well. After being transposed in this manner, the message is transcribed by reading down along each column, making it impossible for anyone who does not know the keyword to translate the message.

A modern computer would be capable of unscrambling such a transmission, even in a situation involving an unknown keyword, but the Allies in World War I were initially unable to break Nebel’s code. However, French artillery captain Georges-Jean Painvin (1886–1980) did succeed in deciphering the code. Though his work was good only for a single day, it enabled the allied armies to counter the German offensive of June 9, 1918.

#### ■ FURTHER READING:

##### BOOKS:

- Haldane, Robert A. *The Hidden War*. New York: St. Martin’s Press, 1978.
- Konheim, Alan, G. *Cryptography: A Primer*. New York: Wiley, 1981.
- Rosen, Kenneth H., and John G. Michaels. *Handbook of Discrete and Combinatorial Mathematics*. Boca Raton, FL: CRC Press, 2000.

##### SEE ALSO

*Codes and Ciphers*  
*Cryptology, History*

## Advanced Photon Source (APS).

SEE *Argonne National Laboratory*.

## AEC (Atomic Energy Commission).

SEE *DOE (United States Department of Energy)*.

## Regis Air Defense System .

SEE *Ballistic Missile Defense Organization, United States*.

## Afghanistan.

SEE *Enduring Freedom, Operation*.

## Aflatoxin

■ JUDYTH SASSOON

Aflatoxins belong to a group of toxins called mycotoxins, which are derived from fungi. In particular, aflatoxins are produced by the soil-born molds *Aspergillus flavus* and *Aspergillus parasiticus* that grow on the seeds and plants. At least 13 aflatoxins have been identified including B1, B2, G1, G2, M1 and M2. The B aflatoxins fluoresce blue and the G aflatoxins fluoresce green in the presence of ultraviolet light. The M aflatoxins are present in milk products. Aflatoxin B1 is the most ubiquitous, most toxic and most well studied of the aflatoxins. *Aspergillus* spp. contamination occurs as a result of environmental stresses on plants such as heat, dryness, humidity or insect infestation. It can also occur if plants are harvested and stored in hot, humid environments. As a result, people who live in the regions of the world most prone to these conditions, sub-Saharan Africa and southeast Asia are at highest risk for aflatoxin poisoning.

Aflatoxins were first discovered in England in 1960 when more than 10,000 turkeys and ducks died within a few months. The disease contracted by these animals was called Turkey X disease and its cause was traced to *Aspergillus flavus* contamination of peanut meal that had originated in Brazil. The toxin was named for the short hand of its causative agent: *A. fla*.

Aflatoxins are the most toxic, naturally occurring carcinogens known. Aflatoxin B1 is an extremely hepatocarcinogenic compound, causing cancer of the liver in humans. Aflatoxin B1 exposure results in both steatosis (an accumulation of fat) and necrosis (cell death) of liver cells. Symptoms of aflatoxicosis are gastrointestinal including vomiting and abdominal pain. Other symptoms can include convulsions, pulmonary edema, coma and eventually death. Aflatoxins also pose a threat to developing fetuses and they are transferred from mother to infant in breast milk. Aflatoxins B1, G1 and M1 are carcinogenic in animals.

Aflatoxin poisoning occurs from ingestion of crops that have been infested with *Aspergillus* spp. or from eating animal products from animals that have ingested these crops. High concentrations of aflatoxins are most often found in plants with very nutritive seeds such as maize, nuts and cereal grains in Africa and rice in China and Southeast Asia. In the United States, peanuts are routinely tested for aflatoxin concentrations, and contamination has also occurred in corn, rice, and cereal grains.

Most consider aflatoxins extremely dangerous and suggest that in human food is only acceptable with no detectable concentration. The maximum allowable concentration of aflatoxins set by the United States FDA is 20 parts per billion (ppb). Foreign markets usually reject grains with concentrations of 4 to 15 ppb. Acceptable levels of aflatoxins for animal consumption are up to 100

ppb. Because of the strict regulations regarding the permissible concentration of aflatoxin, exporting countries often reserve contaminated grains for consumption within their own country. Because *Aspergillus* spp. is usually colorless and does not break down during cooking, it is difficult to know whether or not people are consuming contaminated food.

Evidence exists that Iraq used aflatoxins in biological weapons. In December of 1990, Iraq produced 2,200 liters of aflatoxin, 1,580 liters of which were used in biological warheads. In particular, 16 R400 bombs and 2 Al Hussein (SCUD) warheads were filled with the toxin.

### ■ FURTHER READING:

#### ELECTRONIC:

Aflatoxin—Home Page, "Aflatoxins: Occurrence and Risk" <<http://www.ansci.cornell.edu/plants/toxicagents/aflatoxin/aflatoxin.html>> (March 17, 2003).

Agriculture Network Information Center, "Plant Disease Announcements" <<http://www.agnic.org/pmp/alpha.html>> (March 11, 2003).

World Health Organization: "Hazardous Chemicals in Human and Environmental Health" <[http://www.who.int/pcs/training\\_material/hazardous\\_chemicals/section\\_1.htm#1.2](http://www.who.int/pcs/training_material/hazardous_chemicals/section_1.htm#1.2)> (March 11, 2003).

#### SEE ALSO

*Biological Warfare*  
*Food Supply, Counter-Terrorism*  
*Toxicology*

## Africa, Modern U.S. Security Policy and Interventions

■ JUDSON KNIGHT

United States policy in Africa since World War II has generally been non-interventionist, in the sense that U.S. troops have seldom actually engaged in military or quasi-military activities on the African continent. Exceptions, however, do exist, most notable among them being a limited commitment (both of troops and of covert operatives) during the Congo civil war in the early 1960s, the bombing of Libya in 1986, and the humanitarian mission to Somalia in 1993. More often, the United States has provided assistance to African movements, such as anticommunist guerrillas in Angola during the 1970s and 1980s. America has also used diplomatic and economic pressure, both against South African apartheid in the





Children follow a United States soldier patrolling the Green Line, a heavily contested area in the Somali civil war of the 1980s, during Operation Restore Hope in 1992. ©PETER TURNLEY/CORBIS.

1980s and criminal activities in Nigeria during the twenty-first century.

## Background

After the 1998 embassy bombings in Kenya and Tanzania, the United States conducted bombing raids over both Afghanistan and Sudan, attempting to neutralize Osama bin Laden and his al Qaeda terror network. The fact that the same terrorist group later caused the 2001 bombings in New York City and Washington, D.C., serves to illustrate the fact that events in Africa are not removed from impacting American security and policy. As of July, 2003, the U.S. made a limited troop commitment to secure stability in Liberia and considered a more extensive involvement.

In choosing their policy priorities for Africa, American leaders managed a fine line between appearing interventionist or imperialist on the one hand, and insensitive to Africans' misery on the other. Generally, U.S. policy in Africa has been guided by assessments of the strategic importance of a given nation, its existing alignment or non-alignment with U.S. interests, and the stability of its government.

With the exception of Liberia and Ethiopia, every nation in Africa—more than 50 in all—was at one time a European colony. This is true even in North Africa, whose people are linguistically and culturally distinct from their neighbors to the south. At the beginning of the twentieth century, France held much of west and central Africa; Britain southern and eastern Africa, as well as parts of West Africa; Belgium what is now the Congo, and Portugal a few notable colonies, among them Angola and Mozambique. Germany and Italy, latecomers to African colonialism, controlled some of the sites less rich in natural resources.

In the period between 1945 and 1975, virtually every nation in Africa gained independence, with the Portuguese—first Europeans to colonize in Africa—becoming the last to relinquish colonies. High hopes attended independence, but with few exceptions (a notable one being Botswana), the history of modern Africa has been an unrelieved tale of cruelty, corruption, mismanagement, and rampant disease and poverty. Funds given to help the African people have often ended up in the Swiss bank accounts of dictators, and money intended to build schools and feed children has instead been used to fund civil wars.

## The Congo, Rwanda, and Africa's "First World War"

The Congo exemplified this problem. In 1960, Belgium granted its former colony independence, but this proved only the beginning of new troubles. Civil war ensued, and initially the United States, as a participant in a United Nations (UN) peacekeeping force, seemed to back Prime Minister Patrice Lumumba. But as Lumumba drifted increasingly into the Soviet orbit, the Central Intelligence Agency (CIA) considered means of assassinating him, in the words of the local CIA station chief, "to avoid another Cuba." Meanwhile, the United States provided assistance to army officer Joseph Désiré Mobutu, whose troops captured and killed Lumumba.

Although conditions in the Congo were difficult under Lumumba, they were at least as bad under Mobutu, who became unquestioned leader of the nation in 1966. He renamed the country Zaire and himself Mobutu Sese Seko Kuku Ngbendu wa za Banga, which means "the all-powerful warrior who, because of his endurance and inflexible will to win, will go from conquest to conquest, leaving fire in his wake." For the next three decades, Mobutu, supported by the United States and the World Bank, looted his country, building vast palaces for himself and fattening the pockets of his cronies while the majority of his people lived without electricity, running water, or basic medical care.

Mobutu was overthrown in 1997 by Laurent Kabila, who proved just as corrupt, and who was killed by his own bodyguards in 2001. By then, the Congo had become embroiled in events described collectively as "Africa's First World War." The opening salvo of that larger conflict—a series of conflicts involving Rwanda, the Congo (which returned to its original name in 1997), and other nations—was the infamous Rwandan genocide in 1994.

The conflict involved age-old disputes between the Hutu and Tutsi peoples, who together constitute most of the population in Rwanda, Burundi, and neighboring states. After Rwanda's Hutu dictator, Major General Juvenal Habyarimana, died in a plane crash on April 6, 1994, his supporters blamed the Tutsi-controlled Rwandan Patriotic Front (RPF), and launched a campaign of genocide that resulted in more than 800,000 deaths over a period of a few weeks. By July, the RPF had driven the remnants of the Habyarimana government, along with some 1 million refugees, into neighboring Zaire. This influx served to so destabilize the Mobutu regime that it helped provide the opportunity for Kabila's takeover.

## Somalia, Ethiopia, and Angola: Marxism, Anarchy, and Intervention

The United States was criticized, both at home and abroad, for not intervening in Rwanda, an extremely poor and

landlocked nation with almost no strategic importance to Washington. It is possible that had America intervened, it would have been condemned for interfering in other nations' internal affairs. Such was the case in Somalia just a few months earlier, when U.S. attempts to provide humanitarian assistance so inflamed resentment that even after the terrorist attacks of September, 2001, Muslim critics of U.S. policy would cite Somalia as an example of American imperialism.

Located on the horn of Africa, Somalia also achieved its independence in 1960, and also succumbed to dictatorship, in this case under Major General Mohamed Siad Barre. After overthrowing the government in 1969, Siad Barre launched the country on a disastrous experiment in Soviet-style socialism, complete with posters in the capital city of Mogadishu that featured his face alongside those of Karl Marx and V. I. Lenin. In a country where the principal form of organization is by clan, modern political forms of any kind were foreign, and it would have been difficult to find a more inadequate prescription for Somalia's challenges than Siad Barre's Marxist Leninism.

Ironically, the takeover of neighboring Ethiopia by Communists in 1974 proved Siad Barre's undoing. In the chaos that befell Ethiopia after the downfall of longtime emperor Haile Selassie, Somalia went to war with its neighbor over the Ogaden Desert, and by September, 1977, had all but won. At that point, however, the Soviets switched their allegiance to Ethiopia's Marxist government.

The Soviets' change of allegiance created a strange alliance between Siad Barre and the United States. The proxy war in the Horn of Africa nearly became an entanglement involving U.S. troops, as Zbigniew Brzezinski, National Security Advisor under President James E. Carter, briefly considered deploying the U.S. carrier *Kitty Hawk* to the region in March 1978. The United States and Somalia concluded military agreements in 1980 that allowed U.S. access to naval ports at Mogadishu and other cities.

The military alliance with the United States did not result in any meaningful changes in Siad Barre's style of rule, and over the next decade, his influence slowly declined until he was ousted in 1991. By then, with the Cold War all but finished, the United States—which had strategic naval bases farther south in Kenya—had no particular interest in preventing Somalia from sliding toward anarchy. Then, in 1992, during the last weeks of his administration, President George H. W. Bush committed 25,000 U.S. troops to a UN force involved in distributing famine relief supplies.

Bush was influenced by the fact that the UN had performed well during the crises surrounding the Persian Gulf War of 1990–91, but the experience in Somalia was not to be as successful. By 1993, U.S. forces had become caught in the middle of conflicts between local warlords, and on October 3, 18 U.S. Rangers were killed in a firefight on the streets of Mogadishu. Prior to this debacle, Secretary of Defense Les Aspin had outlined an agenda of

“nation-building” in a nation that had no true government, and in the aftermath of the Mogadishu disaster, Aspin resigned.

Ethiopia and Somalia were just a few of the nations that attempted to apply the Marxist formula to their problems during the 1970s. Numerous other nations aligned with Moscow, but few did so as openly as the former Portuguese colonies of Angola and Mozambique. The United States provided help to the rebels fighting in both countries, though aid to Angola was much greater. In 1985, President Ronald Reagan, under pressure from both the Department of Defense and the CIA, transferred some \$15 million in antiaircraft and antitank missiles to the rebel movement.

The United States commitment to Angola was in part a response to the fact the Soviets and Cubans had become heavily involved on the side of the government, but it was also a product of the magnetism exerted by the rebels’ charismatic leader, Jonas Savimbi. In 1966, Savimbi had formed the National Union for the Total Independence of Angola, known by the initials of its name in Portuguese, UNITA. First he fought against the Portuguese, then against the MPLA (Popular Movement for the Liberation of Angola) when it took control of the government after the Portuguese left. Because the MPLA was aligned with Moscow, Savimbi gained support from a wide array of nations opposed to the Soviet Union: the United States, China, and South Africa. Savimbi managed to convince American conservatives that he was an anti-communist, just as he presented himself to the Chinese as a Maoist. To the regime that maintained the system of apartheid in South Africa, Savimbi’s victory would help keep blacks from getting the idea that they should gain a share of whites’ wealth.

In reality, the war was not about ideology, but about control of the nation’s diamond resources and other natural wealth. The Communist regime of José Eduardo dos Santos was corrupt and cruel, but Savimbi matched its record. In 1989, even Mobutu tried to step in and pressure him to accept a ceasefire. In 1992, with the Cold War over, Savimbi lost U.S. funding. He spent the remainder of his life fighting the government and opposition in his party, looting the populace, and resisting efforts toward peace. Six weeks after his death in February, 2002, the two sides signed a ceasefire agreement.

## Liberia and South Africa: Oppression and Economics

In deciding to intervene, whether by military, economic, or diplomatic means, prudent leaders tend to favor a conservation of resources. An example was America’s response to chaos in Liberia in 1990. The West African nation, founded by freed American slaves in 1847, has proven no more stable or successful than any of its neighbors that had been colonies. Nor has the American influence yet fostered a greater degree of respect for human rights:

ironically, the freed slaves, known as Americo-Liberians, virtually enslaved the native Liberians, who lived under conditions of forced labor and extreme poverty.

Finally, in 1980, Sgt. Samuel K. Doe led a revolt against President William Tolbert, ending 133 years of oppression. Doe, however, proved a tyrant, and he benefited from some \$500 million in U.S. aid even as the quality of life for the Liberian populace continued to decline. When rebels overthrew Doe in 1990, the United States quietly evacuated its diplomatic personnel and other citizens from the troubled nation.

In part because the nation-state is a western construct imposed on Africa, life in post-colonial times has often been characterized by the oppression of one ethnic group by another: first Hutu by Tutsi, then the reverse, first native Liberians by Americo-Liberians, then the reverse, and so on. As most of these situations involved native African ethnic groups, they have attracted little attention in the outside world. By contrast, the regime of apartheid that prevailed in South Africa for more than four decades after 1948, involving as it did oppression of a black majority by a white minority, invoked sharp criticism throughout the western world.

Although many Americans had long condemned apartheid, the issue did not become a part of American popular culture until 1985, as entertainers and college students took up the cause. Activists pressured the Reagan administration to deal aggressively with South Africa, and to isolate the nation economically. In fact the United States did impose a number of economic restrictions on South Africa, but not to a degree demanded by activists. The solutions that worked with recalcitrant U.S. states during desegregation in the 1960s would not necessarily be as successful with an independent nation in the 1980s. Reagan reasoned that while apartheid did not comport with U.S. values, South Africa was of far greater value to the United States than many of its most outspoken critics—among them Zimbabwe, home to the notorious dictatorship of Robert Mugabe.

Reagan’s administration used a combination of limited economic and diplomatic pressure, while allowing South Africans—who at least had a framework of European-style representational government—to work out their own differences. In the end, opposition leader Nelson Mandela was released from prison, apartheid fell, and Mandela became the president of a new South Africa.

## Other Interventions and Non-Interventions

In terms of economic intervention, Sierra Leone and Chad may offer positive examples of what the world community can do to affect policy in Africa. In 2000, the UN imposed a ban on the purchase of diamonds from Sierra Leone, sales of which had been used in large part to fund that nation’s civil war. Two years later, the 11-year war ended in a ceasefire.

Also in 2000, construction began on a pipeline through Chad, an extremely poor country in which oil had been discovered. Rather than permit a repeat of past mistakes, a consortium of companies (including America's Exxon and Mobil), along with the World Bank, devised a strategy to prevent the nation's rulers from misusing funds. Agreements included stipulations that 80% of all oil revenues would be spent on improving health, education, and welfare for the populace. Another 10% would go into escrow accounts for future generations, 5% would be directed toward the local populations in the area of the oil fields, and only 5% would be placed in the hands of the government to do with as it pleased.

**Nigeria: counterfeiting and advance-fee scams.** Another economic and legal battleground—one where problems remain is Nigeria. One of the leading nations in Africa in terms of size and potential wealth, with its oil riches, Nigeria is only slightly more stable than its neighbors, and criminal activity is rampant. The country is particularly notorious for its counterfeiting operations and its business scams.

Nigerian counterfeiting involves not banknotes, but consumer and industrial goods, including garments and textiles, electronics, spare parts, pharmaceuticals, personal products, and even soft drinks. The reason, in part, is that intellectual property owners, frustrated with the national bureaucracy, have done little to put a stop to counterfeiting efforts there. Additionally, owners of rights to these products are often unaware of counterfeiting activities in Nigeria. The Nigerian government has injunctions against these crimes, but has been largely ineffective in pursuing them.

In 1999, years of military rule in Nigeria ended, and U.S. officials took advantage of this opportunity to strengthen law enforcement efforts there. In July, 2002, the two countries signed an agreement for increased law-enforcement cooperation. Part of the agreement was a grant of \$3.5 million from the United States, intended to help Nigeria modernize its police force and provide additional resources to the country's special fraud unit, which targets 419 known scams.

#### ■ FURTHER READING:

##### BOOKS:

- Campbell, Kurt M., and Michele A. Fluornoy. *To Prevail: An American Strategy for the Campaign against Terrorism*. Washington, D.C.: CSIS Press, 2001.
- Haass, Richard, and Meghan L. O'Sullivan. *Honey and Vinegar: Incentives, Sanctions, and Foreign Policy*. Washington, D.C.: Brookings Institution Press, 2000.
- Kissinger, Henry. *Years of Renewal*. New York: Simon and Schuster, 1999.
- Roberts, Brad. *U.S. Foreign Policy after the Cold War*. Cambridge, MA: MIT Press, 1992.

##### ELECTRONIC:

- African Issues. U.S. Department of States. <<http://usinfo.state.gov/regional/af/>> (April 29, 2003).
- Congo Crisis. Maxwell Air Force Base. <<http://www.au.af.mil/au/aul/bibs/congo/congo.htm>> (April 29, 2003).
- USAID in Africa. U.S. Agency for International Development. <<http://www.usaid.gov/regions/af/>> (April 29, 2003).

##### SEE ALSO

- Americas, Modern U.S. Security Policy and Interventions*  
*Egypt, Intelligence and Security*  
*IMF (International Monetary Fund)*  
*International Narcotics and Law Enforcement Affairs (INL), United States Bureau*  
*Kenya, Bombing of United States Embassy*  
*Libya, Intelligence and Security*  
*Libya, U.S. Attack (1986)*  
*Middle East, Modern U.S. Security Policy and Interventions*  
*Morocco, Intelligence and Security*  
*South Africa, Intelligence and Security*  
*Sudan, Intelligence and Security*

## Agent Orange

Agent Orange is a defoliant, that is, a chemical that kills plants and causes the leaves to fall off the dying plants. The name was a code devised by the United States military during the development of the chemical mixture. The name arose from the orange band that marked the containers storing the defoliant.

Agent Orange was an equal mixture of two chemicals; 2, 4-D (2,4, dichlorophenoxy acetic acid) and 2, 4, 5-T (2, 4, 5-trichlorophenoxy acetic acid). Another compound designated TCDD (which stands for 2, 3, 7, 8-tetrachlorodibenzo-para-dioxin) is a by-product of the manufacturing process, and remains as a contaminant of the Agent Orange mixture. It is this dioxin contaminant that has proven to be damaging to human health.

Agent Orange was devised in the 1940s. It was widely used during the 1960s during the Vietnam War. The dispersal of a massive amount of Agent Orange throughout the tropical jungles of Vietnam (an estimated 19 million gallons were dispersed) was intended to deprive the Viet Cong of jungle cover in which to hide.

By 1971, the use of Agent Orange in Vietnam had ended. Even today, however, the damage caused to the vegetation of the region by the spraying of Agent Orange is still visible. Agent Orange applications affected foliage of a diversity of tropical ecosystems of Vietnam, but the most severe damage occurred in the forested coastal areas.

Agent Orange was sprayed over 14 million acres of inland tropical forest. A single spray treatment killed about 10% of the tall trees comprising the forest canopy.

Because Agent Orange herbicide remains in the soil for some time, the contaminant TCDD is quite persistent in soil, with a half-life of three years. (In that period of time, one half of the dioxin originally applied would still be present in the soil.)

Evidence also suggests that the defoliant, and in particular the TCDD dioxin component, is a health threat to soldiers who were exposed to Agent Orange during their tour of duty in Vietnam. Tests using animals have identified TCDD as the cause of a wide variety of maladies. In the mid 1990s, the "Pointman" project was begun in New Jersey, which scientifically assessed select veterans in order to ascertain if their exposure to Agent Orange had damaged them. The project is ongoing. In the meantime, veterans organizations continue to lobby for financial compensation for the suffering they assert has been inflicted on some soldiers by Agent Orange.

## ■ FURTHER READING

### BOOKS:

Gough, M. *Agent Orange: The Facts*. New York: Perseus Books, 1986.

National Academy of Sciences. *Veterans and Agent Orange: Health Effects of Herbicides Used in Vietnam*. Washington, DC: National Academy Press, 1994.

Schuck, P. H. H. *Agent Orange on Trial: Mass Toxic Disasters in the Courts*. Boston: Harvard University press, 1990.

## AI (Army Intelligence).

SEE *INSCOM (United States Army Intelligence and Security Command)*.

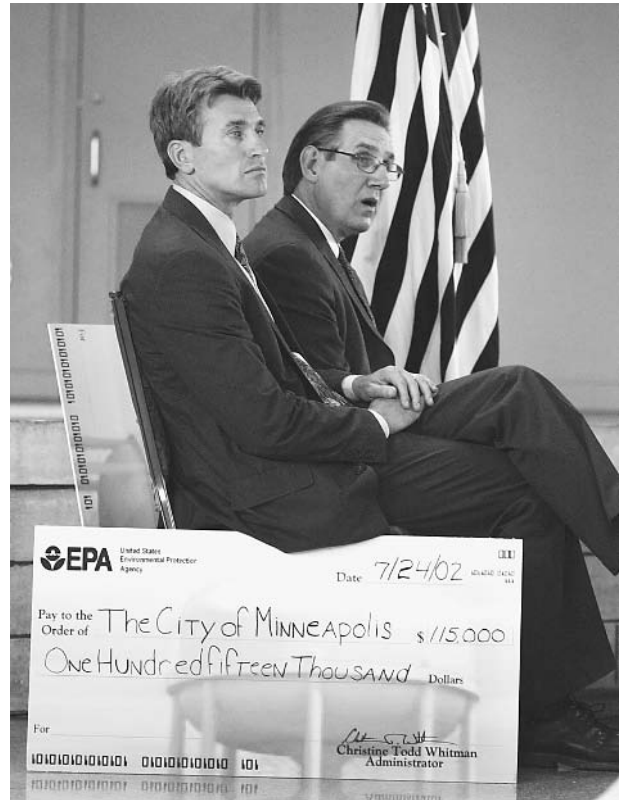
## Air America.

SEE *Vietnam War*.

# Air and Water Purification, Security Issues

■ BRIAN HOYLE

Both water and air are particularly vulnerable to contamination by some bacteria and protozoa, and by their toxic products. Chemicals can also be dispersed in water and by



Minneapolis Mayor R. T. Ryback, left, and St. Paul Mayor Randy Kelly, right, listen during a 2002 meeting where Christine Whitman, head of the Environmental Protection Agency, presented each city with checks for \$115,000 in EPA grants for water security planning. AP/WIDE WORLD PHOTOS.

air. A recent example occurred in 1995, when the Japanese cult Aum Shinrikyo released sarin gas into the Tokyo subway system. The poisonous gas attack killed 12 people and sickened 5,000.

Technologies exist to kill the microorganisms that might be present (disinfection) or to completely remove the microbes and chemicals from the air or water (purification). These technologies, however, are usually designed to remove naturally occurring or polluting contaminants.

Groundwater or surface water treatment focuses on providing water that is fit to drink. Typically, the water is filtered to remove large debris. Some jurisdictions also pass the water through microfilters that remove objects as small as viruses from the treated water. Most drinking water is treated with chlorine or chlorine-containing compounds to kill any bacteria. Other treatments that are gaining widespread acceptance include the use of ultraviolet light, ozone, and other chemicals such as bromine. Water can also be purified by techniques involving reverse osmosis and steam distillation, although these techniques are not typically used, as they are expensive and purify relatively small volumes of water at one time.

Treatment and monitoring ensure that the water emerging from the treatment plant is safe to drink and that

it remains that way all the way to the consumer's tap. However, these measures are not intended to thwart a deliberate act of sabotage. Many of the water treatment and distribution systems in use around the world were built decades ago. Domestic terrorism was virtually unknown at that time, and protective measures were seldom part of the system's design. For example, surface water supplies are often unguarded and exposed (unfenced, etc.).

For large surface water supplies, the volume of water alone makes the possibility of deliberate contamination remote. For example, it has been estimated that the contamination of the Crystal Springs Reservoir that supplies some of the water for San Francisco, California with enough hydrogen cyanide to harm anyone who drinks a glass of water would require over 400,000 metric tons of the poison. Similarly, huge amounts of bacteria or viruses would be required.

Poisoning smaller water sources, particularly after the water has left the treatment plant, is a more realistic possibility. Even if the water has been chlorinated, disease causing microorganisms such as *Giardia* and *Cryptosporidium* are resistant to chlorine, as are bacterial toxins.

More than 100,000 communities in the United States obtain their water from a community well, without the benefit of chlorination or other treatment. Deliberate contamination of these systems could put millions of people at risk.

Another security risk with water supplies involves the nature of monitoring the water. As of 2002, most monitoring techniques for living and nonliving contaminants requires up to 24 hours. "Real time" tests are not routinely available. Thus, contamination would not be detected until long after people had consumed the water.

Air is vulnerable to contamination with a variety of bacteria, viruses, and fungi that are light enough to become dispersed in air currents. When inhaled, the microbes can cause infections. Chemicals and toxins can also float in the air, to be inhaled or settle onto exposed skin.

Air purification has long been possible using filters. Bacteria, viruses, and even some inorganic chemicals can be retained on specialized filters. These filters are mainly suitable for laboratories or relatively small, specifically designed ventilation systems. In large indoor environments such as malls or sizeable office buildings, and in the open air, air purification is virtually impossible.

Contamination of the open air poses a similar problem as the contamination of a large volume of water, namely the amount of poisonous agent that is required. For example, estimates are that hundreds of pounds of anthrax spores would be needed to achieve a massive contamination of the population of a large city.

The release of toxic agents into a more limited area such as an office building is more plausible. Some buildings that are deemed to be a security risk, or which are used for research with highly infectious microbes, are

equipped with safeguards to prevent the spread of airborne infectious agents or poisons. Air treatment, ventilation filters, alarms, and the ability to isolate contaminated zones are usually part of the designed safeguards.

## ■ FURTHER READING:

### BOOKS:

Drell, S. D. *The New Terror: Facing the Threat of Biological and Chemical Weapons*. Stanford, CA: Hoover Institute Press, 1999.

Henderson, D. A., "The Looming Threat of Bioterrorism." *Science* no. 283 (1999): 1279–1282.

Kowalski, W. J., W. P. Bahnfleth, and T. S. Whittam. "Filtration of Airborne Microorganisms: Modeling and Prediction." *ASHRAE Transactions* 105 (1999): 4–17.

O'Toole, T. "Smallpox: An Attack Scenario." *Emerging Infectious Diseases* 5 (1999): 540–546.

### SEE ALSO

*Air Plume and Chemical Analysis*  
*Biological Warfare*

*Environmental Issues Impact on Security*

*Microbiology: Applications to Espionage, Intelligence and Security*

*Water Supply: Counter Terrorism*

---

## Air Force Intelligence, United States

---

### ■ JUDSON KNIGHT

The intelligence-gathering efforts of the U.S. Air Force long predate its establishment as a separate military service in 1947. The Air Force has conducted extensive aerial surveillance, as well as air technical intelligence (ATI) operations—that is, the study of foreign aircraft themselves—since the end of World War I. As time has gone on, equipment and techniques have become more sophisticated, and involvement more widespread. Today's Air Combat Command includes a number of intelligence agencies.

**Background.** The U.S. Air Force has its roots in the Aeronautical Section of the U.S. Signal Corps, founded in 1907, and renamed the Aviation Section in 1914. This became the U.S. Army Air Service in 1918, and the Army Air Corps in 1926. In 1941, on the eve of World War II, the Department of the Army renamed its air section the United States Army Air Force. Two years after the end of World War II, the National Security Act of 1947 for the first time established the Air Force as a separate military service.

Throughout the twentieth century, the air services took part in aerial intelligence, particularly during the Cold



An image ready analyst from the AIA (Air Intelligence Agency) at Lackland Air Force Base, Texas, examines the imagery on a light table taken by a U-2 spy plane. AP/WIDE WORLD PHOTOS.

War and thereafter. In the 1950s, the United States launched one of its most successful spy aircraft, the U-2. Despite the shootdown of pilot Francis Gary Powers over the Soviet Union in 1960, as well as the passage of time and the aging of the craft, the U-2 remained in service during the 1990s. In addition to a number of surveillance craft such as the SR-71 Blackbird, deployed the Vietnam War, the Air Force made extensive use of satellites and unmanned, remotely piloted vehicles.

The Air Force and its predecessors also took a great deal of interest in ATI, which involves the study of aircraft, parts, and accessories. ATI has helped the United States, not only in the building of better aircraft, but also in targeting enemy defense plants for bombing runs. A by-product of ATI work has also been advances in other areas, including computer systems in general, and automatic language translation technology in particular.

**Air intelligence today.** Most air intelligence work today is under the leadership of Air Combat Command (ACC). Headquartered at Langley, Virginia, ACC operates fighter, bomber, reconnaissance, battle-management, rescue, and

theatre airlift aircraft, along with command, control, communication, and intelligence systems. Under its leadership are a number of intelligence-related Air Force activities, most notable of which are the Air Intelligence Agency (AIA) and the Air Force Technical Applications Center (AFTAC).

Established in October 1993, AIA grew out of the Air Force Intelligence Service, established in June 1972. AIA, which is tasked with intelligence collection, security, support for treaty monitoring, and electronic warfare, is headquartered at Kelly Air Force Base (AFB) in Texas. It consists of several components, including the 67th Information Operations Wing and the 690th Information Operations Group at Kelly, as well as the 70th Intelligence Wing at Barksdale AFB in Louisiana. Its three centers are the National Air Intelligence Center at Wright-Patterson AFB in Ohio, the Air Force Information Warfare Center at Kelly, and AFTAC, which it supports administratively, at Patrick AFB in Florida. In the mid-1990s, AIA included 12,600 active-duty personnel, along with 1,900 reservists and 2,400 civilians.

AFTAC is the sole Department of Defense agency operating and maintaining a global network of nuclear

event detection sensors, the U.S. Atomic Energy Detection System (USAEDS). When the USAEDS detects a disturbance in the ground, water, atmosphere, or space, AFTAC laboratories undertake an analysis of the event to discover whether its causes relate to nuclear testing or deployment. It then reports its findings to national command authorities through Air Force headquarters. In the mid-1990s, AFTAC developed the U.S. National Data Center, which makes use of various ground and satellite centers for the monitoring of nuclear activities and treaty compliance worldwide.

## ■ FURTHER READING:

### BOOKS:

- Boyne, Walter J. *Beyond the Wild Blue: A History of the United States Air Force, 1947–1997*. New York: St. Martin's Press, 1997.
- Clancy, Tom. *Fighter Wing: A Guided Tour of an Air Force Combat Wing*. New York: Berkley Books, 1995.
- Gann, Ernest Kellogg. *The Black Watch: The Men Who Fly America's Secret Spy Planes*. New York: Random House, 1989.
- Richelson, Jeffrey T. *The U.S. Intelligence Community*, fourth edition. Boulder, CO: Westview Press, 1999.

### ELECTRONIC:

- U.S. Air Combat Command. <<http://www2.acc.af.mil/>> (April 13, 2003).
- U.S. Air Force Intelligence and Related. Federation of American Scientists. <<http://www.fas.org/irp/agency/usaf/>> (April 13, 2003).
- U.S. Air Intelligence Agency. <<http://aia.lackland.af.mil/>> (April 13, 2003).

### SEE ALSO

- Air Force Office of Special Investigations, United States DoD (United States Department of Defense)*  
*J-Stars*  
*Photographic Interpretation Center (NPIC), United States National*  
*Photography, High-Altitude*  
*USSTRATCOM (United States Strategic Command)*

---

## Air Force Office of Special Investigations, United States

---

The Air Force Office of Special Investigations (AFOSI) is the principal investigative service of the United States Air Force. Established in 1948, AFOSI is charged with investigating and preventing criminal activities by United States Air Force personnel, as well as by individuals outside the air force whose actions threaten the service's equipment,

personnel, activities, or security. Its ranks, which numbered nearly 2,500 in 2002, include active-duty Air Force personnel, reservists, and civilians.

Then United States Secretary of the Air Force W. Stuart Symington formed AFOSI on August 1, 1948, as the result of recommendations by the United States Congress that the air force (created in 1947) consolidate its investigative activities. Symington patterned the new office after the Federal Bureau of Investigation (FBI), and appointed Special Agent Joseph Carroll, assistant to FBI director J. Edgar Hoover, as the first AFOSI chief. Symington and Carroll developed an investigative service designed to provide unbiased information and operate independent of top air force command. To this end, the AFOSI included civilian personnel from the beginning.

AFOSI is based on a fourfold mission, intended to protect the air force from dangers within and without. As stated by AFOSI itself, that mission is to (1) Detect and provide early warning of worldwide threats to the Air Force; (2) Identify and resolve crime impacting Air Force readiness or good order and discipline; (3) Combat threats to Air Force information systems and technologies; and (4) Defeat and deter fraud in the acquisition of Air Force prioritized weapons systems.

**Fulfillment of the AFOSI mission.** The majority of AFOSI activities are directed toward the fulfillment of the second directive listed above. Among the crimes addressed by AFOSI investigators are murder, robbery, rape, drug use and trafficking, black-market activities, and other unlawful acts committed by or against air force personnel. Economic crime, or fraud, is an area of investigation that places particularly large demands on AFOSI resources.

Additionally, the service is concerned with detecting and protecting against outside threats, activities that require investigation of espionage, terrorism, technology transfer, and computer infiltration. In line with the first directive in its mission, AFOSI personnel provide personal protection to senior air force leaders and other officials.

Within the ranks of AFOSI are also personnel with specialized missions and skills who fulfill functions ranging from that of polygrapher to computer expert to behavioral scientist. Other AFOSI agents operate within one of three antiterrorism teams, based at Lackland Air Force Base (AFB) in Texas; Ramstein AFB in Germany; and Hickham AFB in Hawaii.

**Organization, personnel, and training.** In addition to AFOSI headquarters, the organization has eight field investigation regions. Of these, seven are tied with major air force commands: materiel (Region 1), air combat (Region 2), air mobility (Region 3), air education and training (Region 4), United States Air Forces in Europe (Region 5), Pacific Air Forces (Region 6), and Air Force Space Command (Region 8). In line with the original vision of AFOSI as an independent unit, these regions report to AFOSI headquarters and



not to the relevant air force commanders. Finally, there is Region 7, which provides counterintelligence and security-program management under the direction of the Secretary of the Air Force.

As of 2002, AFOSI included more than 160 units worldwide. Its ranks numbered 2,475, with members drawn from active-duty Air Force personnel, reservists, and civilians. The vast majority—1,890 persons—were special agents bearing credentials at the federal level. Each year, the AFOSI, one of the most popular career-field choices in the United States Air Force, welcomed 230 new special agents drawn from active-duty officers and enlisted members, reservists, and civilians.

All members receive 11 weeks of training at the Federal Law Enforcement Training Center in Glynco, Georgia, alongside trainees for other federal law enforcement services. They follow this with another six weeks of training specific to the AFOSI mission. After a one-year probationary period in the field, members typically receive additional training in their given specialties.

#### ■ FURTHER READING:

##### BOOKS:

*DOD Investigation Programs: Background Data.* Washington, D.C.: United States General Accounting Office, 1989.

Wilson, William. *Dictionary of the United States Intelligence Services: Over 1500 Terms, Programs, and Agencies.* Jefferson, NC: McFarland, 1996.

##### ELECTRONIC:

Air Force Office of Special Investigations. <<http://www.dtic.mil/afosi/>> (December 29, 2002).

##### SEE ALSO

*Air Force Intelligence, United States*

---

## Air Marshals, United States

---

United States air marshals are the first police force of the federal government created solely to protect against terrorism. Though they existed in limited numbers prior to the September 11, 2001, terrorist attacks, the signing of the Aviation and Transportation Security Act (ATSA) on November 19 of the same year completely changed the nature of the air marshal program. The ATSA created the air marshals' new employer, the Transportation Security Administration (TSA), and within a little more than a year, several thousand air marshals were on the job. Air marshals perform their job discreetly, and many aspects of the program are deliberately kept secret so as to increase its effectiveness.

## The Changing Face of Flight

At the end of 2001, the federal air marshal program had 33 armed officers, and a budget of about \$4 million. A year later, the number of employees had swelled into the thousands—U.S. officials are reticent, for security reasons, to indicate the number of air marshals that have been deployed—with a budget of more than \$1 billion. The rapid pace of growth was symptomatic of a larger change in the face of air travel after the September 11th attacks. In the aftermath, the federal government placed security screeners under government employment, and planned to put in place a new computerized passenger-profiling system. These were visible signs that the ordinary traveler could hardly fail to notice. Most of all, travelers were confronted with long lines to enter terminals, and with new security rules. Only persons with a ticket were permitted past security checkpoints and into departure gates, and even the most seemingly innocuous items, such as tweezers, were subject to confiscation by security screeners. By January, 2003, all passengers were additionally required to bring luggage intended to be checked into the hold of the aircraft to a screening point for x-ray or other scanning.

**The invisible air marshals.** In contrast to these visible signs of change, there was one change passengers were not likely to notice: the addition of air marshals. In fact, if a marshal's presence on a routine flight was noticed, that meant he (more than 95% of air marshals are male) was not doing his job correctly. A key element of the marshal program is its invisibility, and this is so for a number of reasons, not least of which is the fact that not every flight has a marshal aboard.

At any given moment at the height of business hours, there are approximately 6,000 commercial flights in the air somewhere in the United States. Every day, 25,000 aircraft take off and land, and though the ranks of the marshal program have swelled since September 11, it is not possible to have a marshal on every flight. Officials estimate that even for the highest-priority flights (the determination of which is made by analyzing a number of factors, such as major events that may attract tourist attention), only about 15% had an air marshal on board in the first year after September 11.

**The air marshal's work.** Federal air marshals, known as FAMs, go through a specific procedure when assigned to a flight. They dress in civilian clothes, and before boarding, present their credentials to a ticket agent, who gives them a ticket. Since September, 2001, ticket agents have been trained in this procedure, and are aware of the security precautions involved, which include not drawing any attention to the fact that an FAM is present.

After receiving his ticket, the FAM enters the terminal by special means that allow him to bypass a security



A federal air marshal trainee shoots live rounds during a training session in Egg Harbor Township, New Jersey. Thousands of armed, undercover air marshals have joined the service since the September 11, 2001, terrorist attacks and are flying carefully chosen missions, sometimes on an hour's notice because of new terrorist threats. AP/WIDE WORLD PHOTOS.

check, because he is armed. Once aboard the plane, the crew has knowledge that a marshal is on board, and therefore, he is permitted access to discreetly check all areas of the plane. Federal air marshals are trained to have a variety of ordinary cover stories available to discourage suspicion about repeated movements in different areas of the aircraft, should they become necessary. The Federal air marshal program motto is *Invisus, Inauditus, Impavidus*—unseen, unheard, unafraid.

**Hazards of the job.** In the first year after September 2001, FAMs made a dozen arrests, none of them related to terrorism. They filed about a thousand reports of suspicious activities on planes, but these numbers have shown signs of decreasing as time as passed. Apparently, in the early months, FAMs tended to be overly cautious or overly reactive to potentially dangerous situations, but experience has made them more judicious.

Early assessments of the FAM program suggest that perhaps the greatest routine occupational hazard is a decrease in concentration due to the monotony of being a repeated airline passenger. Flying tends to be taxing enough for civilians who do it regularly, but the FAM does not have the option of going to sleep. Nor is he free to lose

himself completely in a book or magazine article, or an in-flight movie, though he may take part in such activities as a means of blending in. On the one hand, the FAM must try to appear completely ordinary, and on the other, he must be on the alert at all times. Concerned about the effects of flight fatigue on air marshals, the TSA in January, 2003, announced plans to temporarily reassign some FAMs. In order to gain some relief from the boredom and exhaustion of flight, some of these agents would serve in airport terminals, providing surveillance. This announcement elicited considerable criticism, particularly from airport security officials, who complained that the FAMs were most needed in the skies, and that airports were already overstaffed with security personnel.

Issues of training and expertise have also raised concerns about the FAM program. Prior to September 2001, FAMs received 12 weeks' worth of training, but afterward, officials of the Federal Aviation Administration (FAA) and later TSA found themselves faced with a demand to hire and train some 800 FAMs a month. As a result, new recruits found themselves on the job with less than seven weeks' training. Those with previous federal law-enforcement experience might be deployed after as little as a single week of compacted instruction.

In May 2002, as the Senate was considering legislation to allow pilots to carry handguns, TSA director John Magaw testified that the expertise of FAMs was such that pilots did not need to carry guns. However, TSA officials later acknowledged that new recruits had not been required to undergo the rigorous shooting tests required of air marshals prior to September, 2001.

Given the fact that the program had experienced a sudden upsurge in its personnel rolls—equivalent to that of an army mobilizing after a declaration of war—inefficiencies were virtually inevitable. The challenge with which directors of the FAM program were confronted after September, 2001, would have been daunting for any agency, public or private, and thus, the program requires more time before its full effectiveness can be accurately assessed.

#### ■ FURTHER READING:

##### PERIODICALS:

Donnelly, Sally B. "Grounding the Air Marshals." *Time*. 161, no. 4 (January 27, 2003): 17.

Lombardi, Kate Stone. "Air Travel Under a More Watchful Eye." *New York Times*. (January 26, 2003): WC1.

Schneider, Greg, and Sara Kehaulani Goo. "For Air Marshals, a Steep Takeoff." *Washington Post*. (January 2, 2003): A1.

Wald, Matthew L. "New Rule to Limit Boarding Passes from Gate." *New York Times*. (December 10, 2002): A24.

##### ELECTRONIC:

"Armed Air Marshals for UK Flights." British Broadcasting Corporation (BBC) News. <[http://news.bbc.co.uk/1/hi/uk\\_politics/2590309.stm](http://news.bbc.co.uk/1/hi/uk_politics/2590309.stm)> (March 5, 2003).

Transportation Security Administration. <<http://www.tsa.gov/public/>> (March 5, 2003).

##### SEE ALSO

*Aviation Security Screeners, United States Civil Aviation Security, United States FAA (United States Federal Aviation Administration) September 11 Terrorist Attacks on the United States Transportation Department, United States*

## Air Plume and Chemical Analysis

■ BRIAN HOYLE

An air plume is a layer of warm air that immediately surrounds a person's body. It has also been referred to as a human thermal plume.

The skin's surface temperature is typically 33° Celsius, which is approximately nine degrees warmer than

the surrounding air at a typical room temperature. The temperature difference causes heat to be lost from the entire surface of the skin to the surrounding air.

Because warm air rises, the plume rises up the body and flows off the top of the head and shoulders, instead of radiating outward to the surrounding air from all parts of the body. As the air moves up and away from a person, tiny bits of the skin and chemicals that were present on the skin's surface can also be carried upward. The presence of clothing has no effect on the upward movement of the air.

The presence of clothing also does not block the migration of chemicals from items being carried in the clothing. Particles of an explosive in a pocket, for example, will be able to pass through the pores of the fabric to the immediate vicinity of the skin. There, they will encounter the air plume and migrate upward with the airflow.

The chemicals that are carried in the air plume can be detected using sophisticated detection equipment. The chemical analysis of an air plume can detect explosives and even the aromas emitted by microorganisms.

The analysis of an air plume has grown out of studies that relied on the use of what is termed a *schlieren* system. The word *schlieren* is German for streaks, and describes the appearance of air in a special optical system. Schlieren optics measure air flow based on the scattering of light due to differences in density at the interface between moving air and relatively motionless air.

Scientists interested in imaging the *schlieren* patterns produced by people modified the small optical system so that it could be accommodated in a larger device. The device is similar in appearance to the walk through X-ray machines that are now commonplace in airport security areas.

When a subject walks through the portal, the air plume is drawn into an analysis chamber positioned in the portal's archway. Any particles present are collected in a trap. As well, the vapors in the air plume can be condensed onto the trap. Chemical analysis is performed using a machine called an ion trap mobility spectrometer.

The trapping of particles and condensation of the vaporous air plume concentrates any compounds that are present. The trapped sample is delivered to a chamber that converts the sample molecules to ions. Typically, bombarding the sample atoms with electrons accomplishes this conversion. When an electron collides with a sample ion, an electron is dislodged from the sample atom, producing a positively charged ion. As voltage is applied along the length of the chamber, the positively charged sample ions move toward the negatively charged cathode. Separation of the ions occurs based upon their different sizes and masses. For example, smaller ions move down the chamber faster than larger ions. As ions arrive at the cathode, a current is produced. The current can be amplified to produce a detectable signal. The different signals can be plotted to produce a spectrum. The different peaks in the spectrum can be related

to known ions to determine the ionic composition of the sample.

The pattern of the spectrum produced by the nitrate (NO) groups in an explosive such as 2,4,6-dinitrotoluene (TNT) is characteristic of the arrangement of the NO groups within the chemical structure, and is different from the pattern produced by other NO-containing explosives like nitroglycerine, ethylene glycol dinitrate nitroglycerin, cyclotrimethylenetrinitramine, and pentaerythritoltetranitrate.

The spectrometer is extremely sensitive and fast. Chemicals that are present in only a few parts per billion will be detected in about 10 seconds. Thus, even a very small amount of explosive carried in a pocket would register in the spectrometer.

Currently, the chemical analysis of the air plume is geared towards the detection of explosives. The incorporation of other sensors, such as the “electronic nose” that can detect and identify some bacteria based on the unique chemical vapors given off by the cells will enable biological analysis of air plumes in addition to chemical analysis. Incorporating a metal detector into the device could enable one device to be used to screen for conventional, chemical, and biological weapons.

#### ■ FURTHER READING:

##### BOOKS:

Settles, Gary S. *Schlieren and Shadowgraph Techniques*. Heidelberg: Springer-Verlag, 2001.

##### PERIODICALS:

Crabb, C. “Biosensors Enliven the Science of Detection.” *Chemical Engineering* August (1998): 35–39.

Settles, G.S., and W.J. McCann. “Potential for Portal Detection of Human Chemical and Biological Contamination.” *SPIE Aerosense* no. 4378 (2001): paper 01.

##### SEE ALSO

*Air and Water Purification, Security Issues*  
*Biosensor Technologies*  
*Gas Chromatograph-Mass Spectrometer*

## Aircraft Carrier

#### ■ JUDSON KNIGHT

Sometimes characterized as “floating cities,” aircraft carriers are a potent symbol of America’s strength as a superpower. Although nations ranging from the United Kingdom and Russia to Peru and Thailand have their light carrier and helicopter carriers, the large carriers of the United States are without parallel in ability and firepower. Carriers provide an important means of force projection

from the continental United States to any theatre, no matter how hostile, and offer a floating platform for missions that include both combat and intelligence-gathering. As President William J. Clinton said during a visit to the carrier *Theodore Roosevelt* in the 1990s, “When word of crisis breaks out in Washington, it’s no accident that the first question that comes to everyone’s lips is, ‘where is the nearest carrier?’”

### Components in the Carrier Concept

The carrier is one of the leading means for force projection, or the ability to project an aggregation of military personnel from the continental United States (or another theatre) in response to military requirements. As long as it operates in international waters, a carrier needs no permission to conduct landings or overflights. These floating military bases constitute sovereign U.S. territory capable of moving over the oceans—70% of Earth’s surface—in the service of U.S. interests.

Carriers make possible a variety of options. They may be used to insert forces ashore; on the other hand, their presence is so intimidating that they may be used simply to “show the flag,” or remind hostile powers of the U.S. presence. They are capable of attacking airborne, sea borne, or land targets, and engage in sustained operations in support of other forces—for example, the ground forces deployed for Operation Iraqi Freedom in 2003.

**Battle groups and air wings.** National command authorities do not deploy carriers alone. Rather, the carrier is the center of a battle group, a force of a half-dozen or more ships. The carrier battle group, or CVBG, may be used to protect merchant or military shipping; to provide protection to a Marine amphibious source en route to, or arriving in, an objective area; or to establish a naval presence in support of national security interests

Members of a battle group may include at least one destroyer and one frigate, two attack submarines, two guided missile cruisers, one guided missile destroyer, and a logistical support ship. Destroyers and frigates are primarily for anti-submarine warfare, while attack submarines, as their name implies, attack both enemy submarines and ships. Both guided missile cruisers and destroyers are multi-mission surface combatants, the first type armed with Tomahawk cruise missiles for long-range strike capability, and the second equipped for anti-aircraft warfare. The logistical support ship is usually a combined ammunition, oiler, and supply vessel.

Additionally, the carrier—by definition—serves as a home base for a number of aircraft, known as the carrier air wing. These typically include three squadrons of F/A-18 Hornets, which are all-weather fighter and attack aircraft, and one squadron of F-14 Tomcats, made for fleet air defense and precision strikes against ground targets. Along with these are one squadron of S-3B Vikings, the primary overhead/mission tanker, which is equipped for day and



A flight deck crew gives the launch signal as an F/A-18-C Hornet is catapulted off the flight deck of the carrier USS *Kitty Hawk* in the Persian Gulf as part of over 3,000 American sorties flown during Operation Iraqi Freedom. AP/WIDE WORLD PHOTOS.

night surveillance, electronic countermeasures, command/control/communications warfare, and search and rescue; one squadron of EA-6B Prowlers, which jams enemy radar, electronic data links, and communications; one squadron of E-2C Hawkeyes, all-weather tactical warning and control system aircraft; and one squadron of SH-60 Seahawks, twin-engine utility or assault helicopters.

## Overview of a Modern Carrier

U.S. aircraft carriers fall into several groupings, the largest of which is the Nimitz class. Largest warships in the world, these measure 1,092 feet (332.9 m) from bow to stern, and 252 feet (76.8 m) across. As large as it is, the large U.S. carrier still does not provide enough room for takeoff and landing by conventional means; therefore, the carrier deck includes a number of items for these purposes, as well as for the storage of aircraft below decks.

The aircraft do not remain on the carrier's deck when not in use; rather, they rest in a cavernous hangar beneath the deck, to which they can be summoned by means of four deck-edge elevators, each of which is capable of moving two aircraft at a time. For taking off, aircraft are attached to catapults, which give them the necessary acceleration to go from a standing position to 165 miles per hour (265.5 kph) in just two seconds. The flight crew of

the Nimitz-class aircraft carrier is capable of launching two aircraft and landing one every 37 seconds in daylight, or one per minute at night.

The flight crew itself is a choreographed team, or rather a group of teams, each distinguished by jackets of different colors that signify functions. To the pilot in the air, the most critical colors on the deck are the amber and red lights of the Fresnel lenses on deck. Depending on the angle of the light, the pilot knows if he is too low or too high, while red flashing lights automatically signal a wave-off, meaning that the pilot cannot land at that time. When landing, a plane catches an arresting cable using its tailhook, a hook bolted to an 8-foot (2.4 m) bar attached to the rear part of the aircraft. The tailhook can bring a plane from a speed of 150 miles an hour (241.4 kph) to a complete stop within just 320 feet (97.5 m).

Primary Flight Control, or "Pri-Fly," is the control tower for flights. Above it on the "island," the part of the carrier that sticks up above the flight deck, is the bridge, the command and control center of the carrier as a whole. On the bridge is always an officer of the deck (OOD), designated by the ship's commanding officer, who serves a four-hour watch. The OOD is responsible for all facets of the safety and operation of the ship, among which are navigation, ship handling, communications, and routine tests, and inspections. Also on the bridge are the helmsman, who steers the ship, and numerous other personnel.

Powered by two nuclear reactors with four geared steam turbines and four shafts, the Nimitz-class carrier is capable of spending at least half a year at sea, and more than a decade without refueling. Its ship's company exceeds 3,000, with almost 2,500 more on the air wing. Below decks is an entire city, complete with vast warrens of living spaces, dining halls that serve nearly 20,000 meals a day, a radio and television station, a barber shop, a library, gymnasium, a hospital and dentist office, shops, and a post office.

## Evolution of the Carrier

At 11:01 a.m. on January 18, 1911, the U.S. Navy's Eugene Ely landed a Curtiss pusher aircraft on a specially built platform aboard the USS *Pennsylvania*. Thus, was born the concept of the aircraft carrier. On March 20, 1922, the Navy commissioned the *Langley*, its first carrier, built from a converted collier called the *Jupiter*. Later that year, as a result of the 1922 Washington Naval Limitation Treaty, which limited battleship inventories, Congress authorized the conversion of the unfinished battleships *Lexington* and *Saratoga*. In June 1934, the *Ranger*, the first ship built as an aircraft carrier, was commissioned.

During the interwar period, the aircraft carrier benefited from a number of innovations, most of them British in origin. For example, the Royal Navy introduced the idea of arresting wire (originally necessary because the flimsy World War I-era planes might blow overboard), as well as elevator lifts for stowing craft. Later innovations in catapults and landing lights would also come from the United Kingdom. The British and Americans were not the only forces building aircraft carriers; like the Americans, the Japanese, who had signed the Washington naval agreement, converted unfinished battleships to carriers.

Carriers figured heavily in World War II, particularly during operations in the Pacific theatre. The Japanese launched their attack on U.S. forces at Pearl Harbor in December, 1941, from carriers, and in May, 1942, the United States struck back decisively in the Battle of the Coral Sea, the first naval battle in which opposing fleets fought without their ships coming in sight of one another. A month later, the Battle of Midway proved one of the turning points in the war, and reinforced the concept of naval air support.

**Postwar changes.** By the end of World War II, the United States had commissioned more than 34 carriers, with several more made operational late in 1945. But it had also lost several such vessels, including the first two, the *Langley* and the *Lexington*. Following the war, the introduction of guided missiles revolutionized the nature of the carrier battle group, while nuclear fission replaced diesel power for the most advanced carriers.

Several British innovations—the angled landing strip, which made it possible for a jet to land far from parked aircraft, as well as the mirrored landing site and steam

catapults—made it possible to build carriers capable of launching powerful aircraft and managing complex air missions. But as the Cold War progressed, it became clear that only extraordinary carriers could support the vessels' emerging threefold purpose: to deliver air strikes against targets on sea and land; to protect other ships at long range; and to support antisubmarine operations through their battle groups. Only a true world power could afford to build carriers big enough to perform all three tasks—a distinction that, in effect, separated the United States from the rest of the world.

With the launch of its 59th carrier, *Forrestal*, in 1959, the United States introduced the era of the very large carrier. The *Forrestal* included rectangular extensions on the rear part of the flight deck, which greatly expanded the deck area. Designers had also moved the elevators off to the side, so that they could be used even as aircraft were taking off and landing.

Two years later, in 1961, the Navy introduced the first nuclear-powered carrier, the *Enterprise*. It is no accident that the world's most well-known fictional spaceship, from the 1960s television show *Star Trek*, was also called the *Enterprise*. During that era, the standard of excellence among carriers—the epitome of technological superiority anyone was likely to encounter in real life—was the *Enterprise*, which carried 100 aircraft, displaced 75,700 tons (68,674 tonnes), and moved at speeds higher than 30 knots (55.6 kph). With eight nuclear reactors, it could travel for three years before being replaced.

As impressive as it was, the *Enterprise* would be eclipsed by the *Nimitz* (commissioned in May 1975) and the rest of its class. Instead of eight reactors, these required only two, whose uranium cores needed to be replaced once every 13 years. The carriers displaced 81,600 tons, but had much smaller propulsion systems, and thus, could store much more aircraft fuel.

As of 2003, the United States had launched a total of 75 carriers, with two more under construction. Its 12 active carriers included the *Enterprise* and the *Kitty Hawk* class (the *Kitty Hawk* and *Constellation*), all launched in 1961; the *John F. Kennedy*, launched in 1968; and eight carriers of the *Nimitz* class: *Nimitz*, *Dwight D. Eisenhower* (1977), *Carl Vinson* (1982), *Theodore Roosevelt* (1986), *Abraham Lincoln* (1989), *George Washington* (1992), *John C. Stennis* (1995), and *Harry S. Truman* (1998). Additionally, the *Ronald Reagan* was under construction, with launch planned for the middle of the decade, while construction was to begin on the *George H. W. Bush*, with completion planned for 2009. (Both are *Nimitz*-class carriers.)

**Other nations and light carriers.** The United States has decommissioned about as many carriers—63—as the rest of the world had afloat in 2003. Nations with carriers included the United Kingdom, France, Russia, China, Italy, Japan, Spain, India, Brazil, Chile, Peru, China, and Thailand. The leading carrier power, other than the United States, was—not surprisingly, given the many previous

British achievements in carrier design—the United Kingdom. In part to facilitate the building of smaller and more economical carriers, the British in the late 1960s developed the Harrier jet, which takes off almost vertically. As of 2003, its fleet included three small carriers of the *Invincible* class, built for vertical/short takeoff and landing (V/STOL), each capable of carrying eight Harriers and from 10 to 12 helicopters.

France built the *Charles de Gaulle*, a nuclear-powered vessel that could carry 40 planes, as well as the *Jeanne d'Arc* helicopter carrier. The latter type of ship, midway of a carrier and a cruiser, provided a means of giving several nations carrier capabilities. Such was the case with the Russian Federation, which had a large helicopter carrier, the *Gorshkov*, along with a semi-active multi-role carrier, the *Kuznetsov*. As the Soviet Union, Russia was slow to develop carriers, in part because it lacked sufficient ports worldwide. By the late 1960s, however, the Soviets had begun to build aviation cruisers of the *Moskva* class. These have all been decommissioned since then, however. The world's other superpower, China, has a small naval carrier force, consisting primarily of the *Shichang* multi-role support ship.

Other notable naval powers include Italy, which had six carriers, helicopter carriers, or amphibious assault ships either in operation or under construction in 2003. These included the *Andrea Doria*, scheduled for completion in 2007. Built along the V/STOL model, the *Andrea Doria* would hold eight Harriers or 12 helicopters. Other navies with aircraft carriers, helicopter carriers, helicopter destroyers, or amphibious assault ships included Japan, Brazil, India, Spain, Thailand, and Peru.

#### ■ FURTHER READING:

##### BOOKS:

- Clancy, Tom. *Carrier: A Guided Tour of an Aircraft Carrier*. New York: Berkley Books, 1999.
- Kaufman, Yogi. *City at Sea*. Annapolis, MD: Naval Institute Press, 1995.
- Musciano, Walter A. *Warbirds of the Sea: A History of Aircraft Carriers and Carrier-Based Aircraft*. Atglen, PA: Schiffer Publishing, 1994.
- Polmar, Norman. *The Naval Institute Guide to the Ships and Aircraft of the U.S. Fleet*. Annapolis, MD: Naval Institute Press, 1993.
- Preston, Anthony. *Carriers*. New York: Gallery Books, 1993.
- Wooldridge, E. T. *Carrier Warfare in the Pacific: An Oral History Collection*. Washington, D.C.: Smithsonian Institution Press, 1993.

##### ELECTRONIC:

- Haze Gray and Underway World Aircraft Carrier Lists. <<http://www.hazegray.org/navhist/carriers/>> (April 13, 2003).
- U.S. Navy—The Aircraft Carriers. U.S. Navy Office of Information. <<http://www.chinfo.navy.mil/navpalib/ships/carriers/>> (April 13, 2003).

#### SEE ALSO

*Aviation Intelligence, History*  
*E-2C*  
*Libya, U.S. Attack (1986)*  
*National Command Authority*  
*Persian Gulf War*  
*World War I*  
*World War II*

## Airline Security

■ ADRIENNE WILMOTH LERNER

Following the September 11 terrorist attacks on the United States, airline and airport security reform was a key aspect of international anti-terrorist efforts. Although some nations, such as Great Britain and Israel, had created strong passenger and luggage screening protocols before 2001, there were few international standards for airport security. Concern about the possible future use of airplanes in terrorist attacks and hijacking events provoked widespread changes in United States airport security and passenger screening operations.

## United States Aviation and Transportation Security Act

On November 18 and 19, 2001, the United States Congress passed the Airport Security Federalization Act and the Aviation and Transportation Security Act. The laws sought to standardize pre-flight passenger and cargo screening by federalizing security service and screening personnel in the nation's airports. The Aviation and Transportation Security Act created the Federal Transportation Security Administration (TSA) to supervise security operations for sea and air transportation. The TSA hires and trains Federal airport screeners, who under the new law must all be American citizens. Though the acts govern only United States airports, many of the new initiatives and procedures outlined in the legislation have been routine in many foreign airports for several years.

The Aviation and Transportation Security Act also prescribed several fundamental changes in screening and flight protocol beyond the federalization of personnel. As of December 31, 2002, bomb detection devices, which can detect explosive residue, must screen checked baggage. CT Scanning devices and increased hand searching of luggage were among other encouraged reforms.

Passenger screening also increased in scope and effectiveness. Access to airport departure and arrival gates and concourses is now restricted to ticketed passengers.



The renovated American Airlines security checkpoint, part of a \$300 million improvement project, is seen in the American Airlines Terminal 4 of the Los Angeles International Airport. AP/WIDE WORLD PHOTOS.

In addition to the metal detectors already in place in many airports, more careful checks of electronic devices, such as laptop computers and cellular phones, and carry-on luggage, became standard. The Computer Assisted Passenger Prescreening System, a data base system used in conjunction with the Advance Passenger Information System (APIS), provides searchable biographical and security information on air travelers.

New security measures included modifications to aircraft. Fortified cockpit doors, required to remain closed during flight, prevent easy access from the cabin to the cockpit. Pilots and flight crew can now monitor the aircraft cabin with video monitors and recording devices. The Department of Transportation further requires all planes and passenger trains to be equipped with emergency notification systems that are capable of communicating with airport, national, and local "911" emergency services.

Airports themselves are now required to be secured areas. Fences prevent unauthorized entry onto runways and staging areas. Automobiles cannot be left unattended within 300 yards of the airport terminal. Since the September 11, 2001, terrorist attacks on the United States, the number of security personnel and law enforcement officers on duty in the nation's airports has increased. Some

special security details employ K-9 units with chemical and bomb sniffing dogs.

**The new screening process.** Airport security reform mandated several procedural changes that are evident to travelers. Items that were once commonly allowed in carry-on luggage, such as razors and scissors, are now banned in luggage that will be stored in the cabin of a plane. Airports and airlines in the United States now employ a more stringent pre-flight screening process for passengers, as well as luggage.

The first step in the new screening process is to establish, and positively confirm, the identity of the traveler. Travelers must furnish identification that matches itineraries or tickets. If a passenger is traveling to a foreign destination, airlines and security personnel conduct an unseen screening of passengers via the Advance Passenger Information System (APIS), a database that stores biographical information on airline travelers.

After checking-in with the airline, the passenger, and any carry-on luggage, is required to go through a detailed, physical screening. Identification is checked and confirmed for a second time. Travelers must pass successfully through



pulse induction standing or wand metal detectors, while x-ray machines screen baggage. Electronic devices, such as cellular phones, laptop computers, and personal digital assistants (PDAs), are all required to be turned on and shown to security personnel for inspection, or taken out of luggage and screened separately by x-ray. Advanced x-ray machines that transmit images in three colors permit federal screeners to identify organic, inorganic, and metal, items inside of a traveler's baggage. If security personnel are unable to clearly define the contents of a piece of luggage, or suspect prohibited items, then they open the luggage and conduct a hand search. Only passengers and luggage that successfully pass inspection are permitted to proceed to airline departure gates.

Once at the departure gate, airline personnel are required to conduct random security searches as passengers board the plane. These searches are usually brief, but thorough, and involve a hand search of the contents of carry-on luggage. Some passengers are also asked to answer questions regarding their travel plans. These pre-flight searches have received criticism from some who claim that racial and ethnic profiling is the predominant factor in choosing which passengers to search. Others have claimed that the pre-flight screening violates privacy and causes fear with other passengers because the searches are performed in plain sight of fellow travelers. Proponents of the random pre-flight searches assert that they are indeed, random, unless a traveler is flagged by APIS.

As a passenger boards the plane, machines scan boarding cards in order to compile a final passenger manifest. Airline cabin or ground crew then transmits the passenger list to federal aviation and individual airline officials. During the boarding process, passenger identification is sometimes checked for a third and final time.

Baggage that the passenger surrenders to the airline for storage in the cargo hold during flight, or checked baggage, undergoes a different screening process, separate of the passenger. First, baggage is matched to its owning traveler. If the passenger does not board the flight, then the baggage is not loaded onto the plane. This is more easily accomplished with the use of printed, individual, barcode tags affixed to luggage.

Checked baggage screening is geared around the detection of explosive or incendiary devices. X ray machines or computer tomography (CT) scanners screen the content of baggage. CT scanners permit a bag to be x-rayed individually, yet efficiently, and from all sides. The screener also calculates the density and mass of objects within the luggage, checking the data with a database of known mass/densities of dangerous or explosive substances. CT scanners are slower than standard palate x-ray systems that survey several bags at a time, however their screening is more thorough.

**The future of airline security.** Despite general acceptance of most airline and airport security reforms, some programs

remain controversial. Some have criticized the incorporation of law enforcement profiling techniques into routine passenger screening practices, claiming that persons of Middle Eastern ethnicity are more often under suspicion, searched, and detained by security personnel.

The controversy surrounding profiling escalated when officials in the Department of Homeland Security and the Department of Defense proposed the introduction of the Total Information Awareness (TIA) system, a searchable database that stores personal information including financial and medical records. Though the TIA was intended to be used by federal law enforcement officials to collate data and find terrorist networks, Congress severely circumscribed the controversial program in 2003, prohibiting its use for domestic security operations. TIA was later renamed the Terrorist Information Awareness system

With the creation of the United States Department of Homeland Security (DHS), many agencies responsible for airline safety and airport security, including the TSA, were assumed into the new government department. The DHS has combined national anti-terrorist efforts with earlier regulations specifically regarding airports and airlines. The incorporation of the Early Alert System, a color-coded warning system meant to indicate the variable likelihood of terrorist attacks, marked the most notable change in security procedures. As threat levels are elevated, security procedures are heightened. At the Orange and Red levels, airports employ a wider secured perimeter, different flight paths around urban areas, and increased security personnel.

Although TSA is now a part of the Department of Homeland Security, the Department of Transportation and the Federal Aviation Administration (FAA) continue to aid the progress of reforming United States airline security policy through safety recommendations and review of airline practices.

#### ■ FURTHER READING :

##### ELECTRONIC:

Transportation Safety Administration. <<http://129.33.119.130/public/index.jsp>> (12 March 2003).

United States Department of the Treasury. U.S. Customs Service. <<http://www.customs.ustreas.gov/>>(05 January 2003).

##### SEE ALSO

*Air Marshals, United States*  
*APIS (Advance Passenger Information System)*  
*Canada, Counter-terrorism Policy*  
*France, Counter-terrorism Policy*  
*Germany, Counter-terrorism Policy*  
*Israel, Counter-terrorism Policy*  
*September 11 Terrorist Attacks on the United States*  
*United Kingdom, Counter-terrorism Policy*  
*United States, Counter-terrorism Policy*

## Al-Aqsa Martyrs Brigade

The al-Aqsa Martyrs Brigade comprises an unknown number of small cells of Fatah-affiliated activists that emerged at the outset of the current intifadah to attack Israeli targets. It aims to drive the Israeli military and settlers from the West Bank, Gaza Strip, and Jerusalem and to establish a Palestinian state.

**Organization activities.** Al-Aqsa Martyrs Brigade has carried out shootings and suicide operations against Israeli military personnel and civilians and has killed Palestinians that it believed were collaborating with Israel. At least five United States citizens, four of them dual Israeli-U.S. citizens, were killed in these attacks. Intelligence reports claim the group probably did not target U.S. citizens during these attacks. In January 2002, the group claimed responsibility for the first suicide bombing carried out by a female.

The strength of the Al-Aqsa Martyrs Brigade is unknown, and operates mainly in the West Bank and has claimed attacks inside Israel and the Gaza Strip.

### ■ FURTHER READING :

#### ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001, Annual Report: On the record briefing. May 21, 2002 <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17,2003).

U.S. Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

#### SEE ALSO

*Terrorism, Philosophical and Ideological Origins Terrorist and Para-State Organizations Terrorist Organization List, United States Terrorist Organizations, Freezing of Assets*

## Alex Boncayao Brigade (ABB)

The Alex Boncayao Brigade (ABB), the breakaway urban hit squad of the Communist Party of the Philippines New People's Army, was formed in the mid-1980s. The ABB was added to the Terrorist Exclusion list in December 2001. The AAB is responsible for more than 100 murders

and believed to have been involved in the murder in 1989 of U.S. Army Col. James Rowe in the Philippines. In March, 1997, the group announced it had formed an alliance with another armed group, the Revolutionary Proletarian Army (RPA). In March, 2000, the group claimed credit for a rifle grenade attack against the Department of Energy building in Manila and strafed Shell Oil offices in the central Philippines to protest rising oil prices. ABB has approximately 500 members and the largest RPA/ABB groups are on the Philippine islands of Luzon, Negros, and the Visayas.

### ■ FURTHER READING :

#### ELECTRONIC:

CDI (Center for Defense Information), Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <<http://www.cdi.org/terrorism/terrorist.cfm>> (April 17, 2003).

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001," Annual Report: On the record briefing. May 21, 2002 <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17,2003).

U.S. Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

#### SEE ALSO

*Terrorism, Philosophical and Ideological Origins Terrorist and Para-State Organizations Terrorist Organization List, United States Terrorist Organizations, Freezing of Assets*

## Al-Gama'a al-Islamiyya (Islamic Group, IG)

Al-Gama'a al-Islamiyya (Islamic Group, IG) is Egypt's largest militant group, active since the late 1970s, and appears to be loosely organized. IG has an external wing with supporters in several countries worldwide. The group issued a cease-fire in March 1999, but its spiritual leader, Shaykh Umar Abd al-Rahman, sentenced to life in prison in January, 1996, for his involvement in the 1993 World Trade Center bombing and incarcerated in the United States, rescinded his support for the cease-fire in June, 2000. IG has not conducted an attack inside Egypt since August, 1998. Senior members signed Osama Bin Ladin's fatwa in February, 1998, calling for attacks against the

United States. The organization is unofficially split in two factions, one that supports the cease-fire led by Mustafa Hamza and one led by Rifa'i Taha Musa, calling for a return to armed operations. Taha Musa in early 2001 published a book in which he attempted to justify terrorist attacks that would cause mass casualties. Musa disappeared several months thereafter, and there were conflicting reports as to his current whereabouts. The primary goal of the IG is to overthrow the Egyptian government and replace it with an Islamic state, but disaffected IG members, such as those potentially inspired by Taha Musa or Abd al-Rahman, may be interested in carrying out attacks against the U.S. and Israeli interests.

**Organization activities.** The IG has conducted armed attacks against Egyptian security and other government officials, Coptic Christians, and Egyptian opponents of Islamic extremism before the cease-fire. From 1993 until the cease-fire, al-Gama'a launched attacks on tourists in Egypt, most notably the attack in November, 1997, at Luxor that killed 58 foreign tourists. The IG also claimed responsibility for the attempt in June, 1995, to assassinate Egyptian President Hosni Mubarak in Addis Ababa, Ethiopia. The IG has never specifically attacked a U.S. citizen or facility, but has threatened United States interests.

At its peak, the IG probably commanded several thousand hard-core members and a like number of sympathizers, but its present size is unknown. The 1999 cease-fire and security crackdowns following the attack in Luxor in 1997, and more recently, tightened security efforts following the September 11, 2001, terrorist attacks in the United States probably have resulted in a substantial decrease in the group's numbers.

IG operates mainly in the Al-Minya, Asyu't, Qina, and Sohaj Governorates of southern Egypt. They also appear to have support in Cairo, Alexandria, and other urban locations, particularly among unemployed graduates and students, and have a worldwide presence, including the United Kingdom, Afghanistan, Yemen, and Austria.

The organization's external sources of support, if any, are unknown. The Egyptian government believes that Iran, Osama Bin Ladin, and Afghan militant groups support the organization. The IG may also obtain some funding through various Islamic non-governmental organizations.

#### ■ FURTHER READING:

##### ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).  
Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001, Annual Report: On the record briefing. May 21, 2002 <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

#### SEE ALSO

*Terrorism, Philosophical and Ideological Origins Terrorist and Para-State Organizations Terrorist Organization List, United States Terrorist Organizations, Freezing of Assets*

## Al-Ittihad al-Islami (AIAI)

Al-Ittihad al-Islami (AIAI) also operates as, or is known as, the Islamic Union.

AIAI is Somalia's largest militant Islamic organization. AIAI rose to power in the early 1990s following the collapse of the Siad Barre regime. AIAI aims to establish an Islamic regime in Somalia and force the secession of the Ogeden region of Ethiopia. AIAI participates in primarily insurgent-style attacks against Ethiopian forces and other Somali factions. The group is believed to be responsible for a series of bomb attacks in public places in Addis Ababa in 1996 and 1997, as well as the kidnapping of several relief workers in 1998. AIAI sponsors Islamic social programs, such as orphanages and schools, and provides pockets of security in Somalia. AIAI strength is estimated at some 2,000 members, plus additional reserve militias.

The AIAI operates primarily in Somalia, with limited presence in Ethiopia and Kenya. AIAI has received funds from Middle East financiers, Western diaspora remittances, weapons deliveries from Sudan, and—prior to Operation Enduring Freedom—conducted training in Afghanistan with ties to al-Qaeda (also spelled al-Qaida).

#### ■ FURTHER READING:

##### ELECTRONIC:

CDI (Center for Defense Information), Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <<http://www.cdi.org/terrorism/terrorist.cfm>> (April 17, 2003).  
Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).  
Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001," Annual Report: On the record briefing. May 21, 2002 <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).  
U.S. Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

#### SEE ALSO

*Terrorism, Philosophical and Ideological Origins*

*Terrorist and Para-State Organizations  
Terrorist Organization List, United States  
Terrorist Organizations, Freezing of Assets*

## Al-Jama'a al-Islamiyyah al-Muqatilah bi-Libya

Al-Jama'a al-Islamiyyah al-Muqatilah bi-Libya also operates as, or is known as, the Libyan Islamic Fighting Group, Fighting Islamic Group, Libyan Fighting Group, and/or Libyan Islamic Group.

Emerged in 1995 among Libyans who had fought against Soviet forces in Afghanistan, the organization declared the government of Libyan leader Muammar Qadhafi un-Islamic and pledged to overthrow it. Some members maintain a strictly anti-Qadhafi focus and organize against Libyan government interests, but others are aligned with Osama Bin Laden's al-Qaeda (also frequently spelled al-Qaida) organization or are active in the international mujahidin network. Al-Jama'a claimed responsibility for a failed assassination attempt against Qadhafi in 1996 and engaged Libyan security forces in armed clashes during the mid to late 1990s. Currently, the organization engages in few armed attacks against Libyan interests either in Libya or abroad.

Al-Jama'a, operates in Libya, but since late 1990s many members have fled to various Middle Eastern and European countries. The group obtains some funding through private donations, various Islamic non-governmental organizations, and criminal acts.

### ■ FURTHER READING:

#### ELECTRONIC:

CDI (Center for Defense Information), Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <<http://www.cdi.org/terrorism/terrorist.cfm>> (April 17, 2003).

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001," Annual Report: On the record briefing. May 21, 2002 <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

#### SEE ALSO

*Terrorism, Philosophical and Ideological Origins*

*Terrorist and Para-State Organizations  
Terrorist Organization List, United States  
Terrorist Organizations, Freezing of Assets*

## Al-Jihad

Al-Jihad (also known as Egyptian Islamic Jihad, Jihad Group, and Islamic Jihad) is an Egyptian Islamic extremist group active since the late 1970s. Al-Jihad merged with Osama Bin Ladin's al-Qaida organization in June, 2001, but may retain some capability to conduct independent operations. Al-Jihad continues to suffer setbacks worldwide, especially after tightened Egyptian security in the aftermath of the September 11, 2001 terrorist attacks in the United States. Al-Jihad's primary goals are to overthrow the Egyptian government and replace it with an Islamic state, and to attack U.S. and Israeli interests in Egypt and abroad.

**Organization activities.** Al-Jihad specializes in armed attacks against high-level Egyptian government personnel, including cabinet ministers, and car-bombings against official U.S. and Egyptian facilities. The original Jihad was responsible for the assassination in 1981 of Egyptian President Anwar Sadat. The organization claimed responsibility for the attempted assassinations of Interior Minister Hassan al-Alfi in August 1993 and Prime Minister Atef Sedky in November 1993. As of May, 2002, Al-Jihad has not conducted an attack inside Egypt since 1993 and has never targeted foreign tourists there. Al-Jihad is responsible for the Egyptian embassy bombing in Islamabad in 1995; in 1998 an Al-Jihad attack against U.S. Embassy in Albania was thwarted.

The actual size of Al-Jihad is unknown, but the organization has at least several hundred hardcore members. Al-Jihad operates in the Cairo area, but most of its network is outside Egypt, including Yemen, Afghanistan, Pakistan, Lebanon, and the United Kingdom, and its activities have been centered outside Egypt for several years.

The Egyptian government claims that Iran supports Al-Jihad. Its merger with al-Qaeda also boosts Osama Bin Ladin's support for the group. Al-Jihad also may obtain some funding through various Islamic non-governmental organizations, cover businesses, and criminal acts.

### ■ FURTHER READING:

#### ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. *Patterns of Global Terrorism 2001, Annual Report: On the record briefing*. May 21, 2002 <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. *Annual reports*. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

#### SEE ALSO

*Terrorism, Philosophical and Ideological Origins Terrorist and Para-State Organizations Terrorist Organization List, United States Terrorist Organizations, Freezing of Assets*

## Allied Democratic Forces (ADF)

The Allied Democratic Forces (ADF) is a diverse coalition of a few hundred fighters from the National Army for the Liberation of Uganda (NALU), Islamists from the Salaf Tabliq group, Hutu militiamen, and fighters from ousted regimes in Congo. The conglomeration of fighters formed in 1995 in opposition to the government of Ugandan President Yoweri Museveni. The ADF seeks to use the kidnapping and murder of civilians to create fear in the local population and undermine confidence in the government. The group is suspected to be responsible for dozens of bombings in public areas. A Ugandan military offensive in 2000 destroyed several ADF camps, but ADF attacks continued in Kampala in 2001.

ADF operates in western Uganda and eastern Congo. ADF has received funding, supplies, and training from the government of Sudan and perhaps from sympathetic Hutu groups.

#### ■ FURTHER READING:

##### ELECTRONIC:

CDI (Center for Defense Information), *Terrorism Project*. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <<http://www.cdi.org/terrorism/terrorist.cfm>> (April 17, 2003).

Central Intelligence Agency. *World Factbook, 2002*. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001," *Annual Report: On the record briefing*. May 21, 2002 <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. *Annual reports*. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

#### SEE ALSO

*Terrorism, Philosophical and Ideological Origins Terrorist and Para-State Organizations Terrorist Organization List, United States Terrorist Organizations, Freezing of Assets*

## Al-Qaeda (also known as Al-Qaida)

Responsible for the September 11, 2001, terrorist attacks upon the United States, Al-Qaeda (also known as Al-Qaida) was established by Osama bin Ladin (also spelled Usama Bin Ladin or Osama bin Laden) in the late 1980s to bring together Arabs who fought in Afghanistan against the Soviet Union. Al-Qaeda helped finance, recruit, transport, and train Sunni Islamic extremists for the Afghan resistance. Al-Qaeda's current goal is to establish a pan-Islamic Caliphate by working with allied Islamic extremist groups to overthrow regimes it deems "non-Islamic" and expelling Westerners and non-Muslims from Muslim countries. Al-Qaeda has issued statement under banner of "The World Islamic Front for Jihad against the Jews and Crusaders" in February 1998, saying it was the duty of all Muslims to kill U.S. citizens—civilian or military—and their allies anywhere in the world. The World Islamic Front for Jihad merged with Egyptian Islamic Jihad (Al-Jihad) in June 2001.

**Organization activities.** On September 11, 2001, 19 al-Qaeda suicide attackers hijacked and crashed four U.S. commercial jets, two into the World Trade Center in New York City, one into the Pentagon near Washington, D.C., and a fourth into a field in Shanksville, Pennsylvania, leaving about 3,000 individuals dead or missing. Al-Qaeda also directed the October 12, 2000 attack on the U.S.S. *Cole* in the port of Aden, Yemen, killing 17 U.S. Navy crewmembers, and injuring another 39. Al-Qaeda also admitted responsibility for the bombings in August 1998 of the U.S. embassies in Nairobi, Kenya, and Dar es Salaam, Tanzania, that killed at least 301 individuals and injured more than 5,000 others. Al-Qaeda claims to have shot down U.S. helicopters and killed U.S. servicemen in Somalia in 1993 and to have conducted three bombings that targeted U.S. troops in Aden, Yemen, in December 1992.

Al-Qaeda is linked to unrealized plans to assassinate Pope John Paul II during his visit to Manila in late 1994; a plan to kill President Clinton during a visit to the Philippines in early 1995; the planned midair bombing of a dozen U.S. trans-Pacific flights in 1995; and plans to set off a bomb at Los Angeles International Airport in 1999. They



An Air Force RQ-1 Predator pilotless aircraft, capable of launching Hellfire air-to-ground missiles in CIA operations similar to the pin-point missile strike that killed Qaed Salim Sinan al-Harethi, a top al-Qaeda operative, in Yemen on November 4, 2002. AP/WIDE WORLD PHOTOS.

also plotted to carry out terrorist operations against U.S. and Israeli tourists visiting Jordan for millennial celebrations in late 1999. (Jordanian authorities thwarted the planned attacks and put 28 suspects on trial.) In December, 2001, suspected al-Qaeda associate Richard Colvin Reid attempted to ignite a shoe bomb on a transatlantic flight from Paris to Miami.

Al-Qaeda may have several thousand members and associates in cells located around the world, and also serves as a focal point or umbrella organization for a worldwide network that includes many Sunni Islamic extremist groups, some members of al-Gama'a al-Islamiyya, the Islamic Movement of Uzbekistan, and the Harakat ul-Mujahidin.

Al-Qaeda has cells worldwide and is reinforced by its ties to Sunni extremist networks. Coalition attacks on Afghanistan since October 2001 have dismantled the Taliban—once al-Qaeda's protectors—and led to the capture, death, or dispersal of al-Qaeda operatives. Al-Qaeda members at large, including as of April 2003, Osama bin Ladin, have vowed to attempt to carry out future attacks against U.S. interests.

Bin Ladin, member of a billionaire family that owns the Bin Ladin Group construction empire, is said to have

inherited tens of millions of dollars that he uses to help finance the group. Al-Qaeda also maintains moneymaking front businesses, solicits donations from like-minded supporters, and illicitly siphons funds from donations to Muslim charitable organizations. U.S. efforts to block al-Qaeda funding has hampered their ability to obtain money.

#### ■ FURTHER READING:

##### ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001, Annual Report: On the record briefing. May 21, 2002 <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

##### SEE ALSO

*Terrorism, Philosophical and Ideological Origins Terrorist and Para-State Organizations*

*Terrorist Organization List, United States  
Terrorist Organizations, Freezing of Assets*

## Americas, Modern U.S. Security Policy and Interventions

■ JUDSON KNIGHT

In 1823, the Monroe Doctrine provided a framework for United States security policy in the Americas by declaring the Western Hemisphere under a U.S. “sphere of influence”. This served to warn away European colonial powers, while providing justification for U.S. intervention in the affairs of nations throughout Central and South America and the Caribbean. The Monroe Doctrine, along with other statements of policy by modern U.S. presidents, served as a basis for actions against Communist influence in Cuba, Nicaragua, Grenada, and other countries. As the Cold War drew to a close, U.S. action in Latin America, including the invasion of Panama in December 1989, tended to focus on anti-drug activities.

### U.S. Policy and Interventions, 1823–1946

President James Monroe issued his famous doctrine in a speech before Congress. In response to rumors of a planned Franco-Spanish action to restore Spain’s empire in the New World, Britain had made overtures to the United States for a joint policy opposing international intervention in the Americas. Former presidents Thomas Jefferson and James Madison urged Monroe to accept the British offer. However, Monroe’s secretary of state, future president John Quincy Adams, advised him instead to make a unilateral statement of U.S. interests in the Americas—interests so great that outside intervention would meet with swift military action.

The Monroe Doctrine was to be a basis for a range of activities, from direct military intervention to support of friendly regimes, and from protection of Latin American nations against European aggression to humanitarian assistance for the peoples of Latin American countries. It was also the basis for American isolationism with regard to events overseas. Significantly, the United States, whose first international action was against Libyan pirates during Jefferson’s administration, would not again be involved in overseas military activity until the Spanish-American War of 1898—itself fought primarily over Cuba and Puerto

Rico. Even in 1917, the nation entered World War I partly on the basis of information that Germany intended to foment an attack against the United States through Mexico.

Mexico was the target of the first U.S. military action in the Americas, whereby the nation acquired much of what is now the southwestern United States in 1846. During the 1850s, the United States intervened repeatedly in Nicaragua, which U.S. adventurer William Walker ruled as a private colony for two years. The 1855–57 occupation by mercenaries under Walker, who was from Tennessee, later sparked southern hopes of a Confederate empire in Latin America.

Following the Spanish-American War, the United States gave Cuba its independence, but included in the Cuban constitution the Platt Amendment (1901), whereby it reserved the right to intervene in Cuba. In 1903, Washington backed the revolt of Panama against Colombia, which enabled the United States to begin building the Panama Canal. The years from 1904 to 1945 saw literally dozens of covert or military interventions in Cuba, the Dominican Republic, Guatemala, Haiti, Honduras, Mexico, Nicaragua, and Panama. These involved protection of U.S. facilities and personnel, U.S. businesses such as the United Fruit Company in Guatemala, and pro-American governments.

Particularly notable was the action against Mexican guerrilla leader Pancho Villa, whose 1916 raid on the city of Columbus, New Mexico, killed 17 Americans, the greatest loss of civilian life due to foreign action on U.S. soil between 1812 and 2001. American troops, led by General John Pershing, pursued Villa, but failed to catch up with him before they were diverted to Europe.

U.S. forces repeatedly intervened in Nicaragua to shore up pro-American governments, and, in 1926, to fight back a putative Bolshevik conspiracy. This was the leftist nationalist movement of Augusto César Sandino, whose name a later generation of guerrillas would adopt for their movement. The United States in 1929 created a military academy to train Nicaragua’s National Guard, under the leadership of Anastasio Somoza García. In 1934, Somoza had Sandino assassinated, and in 1936, he assumed the presidency. His family would control the nation until the Sandinistas took power in the late 1970s.

As these events were taking place in Nicaragua, the United States was intervening in another nation destined to become communist, Cuba. In 1933, President Franklin D. Roosevelt sent warships to quell unrest, and ultimately helped install the government of Fulgencio Batista. A year later, the Platt Amendment was repealed. Batista would rule until 1959, when he was overthrown by Fidel Castro.

In the intervening years, the United States sought to keep Axis and Communist influence out of Latin America. Its opposition to outside invaders influenced support of military leaders, who tended to establish more stable, if less popular, regimes than did liberal democrats. The United States supported the creation of National Guard-style forces in Haiti and the Dominican Republic, and in

1946, established the U.S. Army School of the Americas in Panama. The school, which would provide military training to a generation of leaders, taught its students that the chief threat to a nation is internal subversion—i.e., leftist revolts.

## U.S. Policy and Interventions, 1946–81

When the leftist regime of President Jacobo Arbenz Guzman seized control of United Fruit properties in Guatemala in 1954, the U.S. Central Intelligence Agency (CIA) began activities against him, training opposition forces in Honduras. Arbenz's purchase of arms from Czechoslovakia only heightened U.S. fears of Communist subversion. The CIA-backed paramilitary force overthrew his regime, replacing him with Carlos Castillo Armas, a leader more favorable to U.S. interests.

Such actions won the United States little support, but Washington's principal desires for the Americas were stability and protection of U.S. economic and strategic interests. If the United States could achieve this by supporting democratic movements and opposing dictatorships, it would, as it did when the administration of Ronald Reagan backed Jose Napoleon Duarte in El Salvador during the 1980s, or when that of George Bush deposed Manuel Noriega in Panama in 1989.

More often than not, however, military leaders—even those who seized power by coups—tended best to serve U.S. needs. President-elect John F. Kennedy articulated this fact in 1960, after right-wing forces seized power in El Salvador, when he noted that "Governments of the civil-military type of El Salvador are the most effective in containing communist penetration in Latin America."

**Castro and Cuba.** Castro's assumption of power in Cuba presented Washington with a nightmarish scenario. Not only was it presented with a pro-Moscow regime just 90 miles from Miami, but Castro—despite his unflinching support for Soviet policy—managed to position himself as a freedom-loving nationalist rather than a communist. Furthermore, he was a charismatic figure, who has continued to enjoy strong support among some U.S. intellectuals and entertainers.

In 1960, President Dwight D. Eisenhower authorized the CIA to undertake covert actions against Castro. Much of what followed, courtesy of a predecessor to the agency's Directorate of Science and Technology, ventured into the territory of the ridiculous: exploding cigars, poisoned milkshakes, powder that would cause the dictator's famous beard to fall off. In April, 1961, the United States sent in a force of 1,400 anti-Castro Cubans, who landed at Cuba's Bahía de los Cochinos, or Bay of Pigs. The venture turned into a rout, and gave Castro a huge public-relations victory.

A Soviet missile buildup in Cuba in October, 1962, prompted the Cuban Missile Crisis, bringing the United States close to nuclear war with the Soviet Union. The incident highlighted the degree to which Castro was a thorn in Washington's side, and throughout the 1960s, the United States conducted covert sabotage campaigns against Castro. It also maintained an economic embargo, and kept a close watch on Cuba from the naval base at Guantanamo Bay—a strategic piece of property retained by the United States when Cuba gained its independence decades earlier.

**Dominican Republic, Chile, and the Panama Canal.** From the 1960s to the 1980s, the United States opposed communist and pro-communist movements in several countries. President Lyndon B. Johnson, claiming threatened communist subversion, invaded the Dominican Republic in 1965. In Chile in 1973, the administration of President Richard M. Nixon, operating through the CIA, supported a coup led by the right-wing General Augusto Pinochet against the Marxist president, Salvador Allende. Allende died, either by suicide (according to Pinochet) or by murder (according to Allende's supporters).

Like Castro, Pinochet imprisoned and tortured opponents, suppressed free speech, and maintained a strong military presence throughout the country. Unlike Cuba, however, Chile—on the brink of economic collapse under Allende—prospered under Pinochet, who imposed free-market reforms. Pinochet, who later submitted to free elections and was voted out of office, is one of the most oft-cited examples, both by critics and supporters of U.S. policy, of a U.S.-supported dictator in Latin America.

The administration of President James E. Carter sought to shift from the U.S. tradition of support for right-wing regimes, and cut off aid to the dictatorships in Guatemala and Nicaragua. Carter undertook negotiations to return the Panama Canal to Panama, and did not attempt to intervene when the Sandinistas removed a later Somoza from power and established a pro-Moscow regime in Nicaragua in 1979.

## U.S. Policy and Interventions, 1981–Present

President Ronald Reagan reversed this trend. In October, 1983, he launched Operation Urgent Fury, the first significant U.S. military action since Vietnam, on the Caribbean island of Grenada. Grenada had become a pro-Soviet dictatorship in 1979—President Maurice Bishop even called his cabinet a "politburo"—but neither the Carter nor the Reagan administration sought to disrupt its government.

Tensions rose, however, when Cuban military personnel began building an airport capable of accommodating large Soviet bombers. In 1983, Bishop's minister of



defense launched a coup, killing Bishop and half the politburo, including the minister of education, who was pregnant. After the new dictator placed the entire island under house arrest, Reagan sent in the military to protect some 600 U.S. students and other citizens there.

**El Salvador.** Meanwhile, the Reagan administration had become involved in another tiny country, El Salvador, which was caught in a battle between the Marxist FMLN, the right-wing ARENA Party under Roberto d'Aubisson, and the Christian Democrats under Duarte. The FMLN enjoyed considerable support from U.S. leftists, who claimed that Washington was backing d'Aubisson.

Ironically, throughout the period from 1982 to 1984, the CIA was funneling money into efforts in favor of Duarte and against d'Aubisson. For example, when European journalists visited the country in 1983, the CIA provided them with negative information on the right-wing leader. Despite the fact that Washington backed the liberal regime, El Salvador remained fraught with problems, as rightist and leftist death squads battled over the country. In 1989, Duarte was voted out in favor of an ARENA candidate.

**Nicaragua.** The Reagan administration provided considerably more support for efforts against a regime openly aligned with the Kremlin: the Sandinistas in Nicaragua. U.S. actions in Nicaragua were closely tied with undertakings in neighboring countries, and one of Reagan's aims was to keep the Sandinistas from exporting their revolution. In this, he would be strongly opposed by congressional Democrats, and by U.S. intellectuals and entertainers, many of whom visited Nicaragua and proclaimed their support for the regime.

Beginning in 1981, the CIA began training a number of anti-Sandinista groups, collectively known as *Contras*, and sponsored the production of two training manuals, *Freedom Fighters Manual* and *Psychological Operations in Guerrilla Warfare*. When these manuals later became public, their contents prompted an outcry against CIA tactics, leading to an internal investigation.

The agency also conducted its own efforts against the regime in Managua, despite the Boland Amendment to the War Powers Act of 1973, passed by Congress in December 1982. Boland prevented the CIA or Department of Defense from using funds to overthrow the Nicaraguan government. In 1984, Congress passed a second Boland Amendment in response to the CIA mining of harbors on Nicaragua's Atlantic and Pacific coasts. In 1986, however, Congress appropriated \$70 million in aid for the Contras. (The Boland Amendment was later repealed.)

At the same time, the Reagan administration and the CIA became involved in an effort to sell weapons to Iran, secure the release of hostages in Lebanon, and divert

funds to the Contras. A pro-Syrian newspaper in Lebanon broke the story of Iran-Contra in November 1986, and for many months thereafter, the administration would be caught up in the scandal. Thanks to support for the Contras, combined with reductions in Soviet aid to the Sandinistas, the two sides signed a ceasefire agreement in 1987. The Contras agreed to free elections in February 1990, and these resulted in the election of Violeta Chamorro, a member of the liberal democratic opposition.

**Panama and Haiti.** Although opponents of U.S. policy in Latin America cite early CIA alliances with Noriega, for most of his career as Panamanian dictator, Noriega was openly opposed to the United States and closely aligned with Castro. He was also involved in drug trafficking, for which he was indicted by a Florida grand jury in February, 1988.

In 1989, President H. W. Bush invested \$10 million in clandestine radio broadcasts against Noriega, and in December launched Operation Just Cause. The operation, which involved 27,000 U.S. troops, was at the time the largest U.S. military undertaking since Vietnam. Its stated goals were the protection of the Panama Canal and the 35,000 U.S. citizens living in Panama, as well as the removal of Noriega himself, promoting democracy, and bringing an end to drug activities in the country. The operation resulted in Noriega's capture and trial.

Less clear were the results of a military operation in Haiti, undertaken by the administration of William J. Clinton in 1994. The purpose was to restore President Jean-Bertrand Aristide, who had been deposed by a military coup, and in that regard, the operation was successful. However, political, economic, and social conditions on the troubled island continued to erode, and in March, 1999, the remaining U.S. forces departed the island amid continuing instability.

**The war on drugs.** From Reagan's time onward, the United States has been involved in the war on drugs to stop the flow of cocaine, marijuana, and other narcotics from Colombia, Peru, Bolivia, and other countries. The U.S. Drug Enforcement Administration (DEA) has been, and continues to be, involved in this war, as is the CIA. The CIA has undertaken cooperative efforts with the governments of Colombia and Peru to interdict drug traffickers. Part of this program is an airborne initiative whereby CIA and national air force personnel shoot down aircraft whose pilots refuse to identify themselves. In many regards, these efforts have been successful, and helped to reduce the flow of drugs; however, in April 2001, miscommunications resulted in the Peruvian shootdown of a plane carrying a U.S. missionary family. The mother and her seven-month-old daughter were killed.

In the post-Cold War environment, drug gangs are a much greater threat to stability in Latin America than are

revolutionaries, although these are often linked. With the elimination of support from Moscow, leftist groups such as Colombia's FARC rebels have turned to kidnapping Americans, Europeans, and Japanese, and holding them for ransom. The same was the case with Peru's Tupac Amaru, which held prisoners at the Japanese embassy in Lima for several months before Peruvian forces stormed the building in early 1997.

Many of these groups make common cause with drug cartels, and some are directly involved with the drug trade. Such was the case with Peru's Sendero Luminoso, or "Shining Path," which, with its Maoist ideology, never accepted aid from Moscow. Instead, it supported itself largely through cocaine trafficking. Sendero was largely neutralized with the capture of its leader, Abimael Guzman, in 1992. The early 1990s also saw the death of Colombian cocaine lord Pablo Escobar and the capture of his associate Carlos Lehder, as well as international terrorist Carlos "the Jackal" Ramirez.

#### ■ FURTHER READING:

##### BOOKS:

- Bouvier, Virginia Marie. *Whose America? The War of 1898 and the Battles to Define the Nation*. Westport, CT: Praeger, 2001.
- Gilderhus, Mark T. *The Second Century: U.S.-Latin American Relations Since 1889*. Wilmington, DE: Scholarly Resources, 2000.
- Hillman, Richard S., John A. Peeler, and Elsa Cardozo da Silva. *Democracy and Human Rights in Latin America*. Westport, CT: Praeger, 2002.
- Musicant, Ivan. *The Banana Wars: A History of United States Military Intervention in Latin America from the Spanish-American War to the Invasion of Panama*. New York: Macmillan, 1990.
- Richelson, Jeffrey T. *The U.S. Intelligence Community*, fourth edition. Boulder, CO: Westview Press, 1999.
- Sicker, Martin. *The Geopolitics of Security in the Americas: Hemispheric Denial from Monroe to Clinton*. Westport, CT: Praeger, 2002.
- Szumski, Bonnie. *Latin America and U.S. Foreign Policy: Opposing Viewpoints*. St. Paul, MN: Greenhaven Press, 1988.

##### SEE ALSO

*Argentina, Intelligence and Security*  
*Bay of Pigs*  
*Brazil, Intelligence and Security*  
*Bush Administration (1989–1993), United States National Security Policy*  
*Chile, Intelligence and Security*  
*Colombia, Intelligence and Security*  
*Cuba, Intelligence and Security*  
*Cuban Missile Crisis*  
*Customs Service, United States*  
*DEA (Drug Enforcement Administration)*  
*Drug Control Policy, United States Office of National*

*Drug Intelligence Estimates*  
*El Salvador, Intelligence and Security*  
*FBI (United States Federal Bureau of Investigation)*  
*Guatemala, Intelligence and Security*  
*International Narcotics and Law Enforcement Affairs (INL), United States Bureau*  
*Kennedy Administration (1961–1963), United States National Security Policy*  
*Mexico, Intelligence and Security*  
*National Drug Threat Assessment*  
*NDIC (Department of Justice National Drug Intelligence Center)*  
*Nicaragua, Intelligence and Security*  
*Panama Canal*  
*Peru, Intelligence and Security*  
*Reagan Administration (1981–1989), United States National Security Policy*  
*Spanish-American War*

## Ames (Aldrich H.) Espionage Case

■ ADRIENNE WILMOTH LERNER

A 31-year veteran of the Central Intelligence Agency, Aldrich "Rick" Hazen Ames became famous in 1994 as the highest paid "mole" (double agent) in United States history. Ames made millions of (US) dollars for information he provided to the Soviet KGB, and later Russian intelligence, while a mid-level employee of the CIA. The information he sold to the KGB included the names of Russian double agents and operatives working for the U.S. within the Soviet intelligence community, ultimately leading to their capture, imprisonment, or execution by Soviet authorities. Ames was thus, one of the most destructive double agents to compromise the security of the United States intelligence services.

A decade after Ames was born in 1941, his father, a college professor, gained employment as a CIA analyst. Ames attended college at George Washington University, majoring in history. He began working for the CIA in 1959 while still a student, largely because of his father's position there.

Ames's performance throughout his career at the CIA was marked by mediocrity. He continued to be promoted, but never attained routine access to the highest level of classified materials. Ames made his first deal with the Soviets in April, 1985, selling CIA secrets for an initial payment of \$50,000. Later that year, Ames was sent to Mexico City to recruit new agents. One of his first recruits was a woman with whom he was having an affair, Colombian cultural attaché Maria Del Rosario Casas. Ames married Casas later that year. She aided Ames in his illegal activities.



The CIA and FBI significantly delayed the detection of CIA turncoat Aldrich Ames, shown handcuffed, by failing for five years to mount a serious, joint investigation into their loss of Russian agents from 1956 to 1986. AP/WIDE WORLD PHOTOS.

The CIA transferred Ames to Rome in 1986, where he stayed until 1988 working for the CIA's Soviet Counterintelligence Division, at the same time selling secrets to the KGB. Although Ames's job was allegedly to recruit Soviet agents (from the embassy in Rome) into the CIA, he failed to successfully recruit a single Soviet agent. His work, however, provided him with the names of Soviet informants and it was this information he sold to the KGB. By 1989, after his return to the United States, he had made enough money to pay cash for a \$540,000 home in Arlington, Virginia, an exclusive suburb of Washington, D.C., and another \$100,000 for improvements on the house. He told friends and acquaintances he and his wife had inherited money from her family in Colombia.

In 1991, Ames was transferred to the CIA's Counter-narcotics Division. Although he no longer had authorized access to information his Russian handlers might want, he managed to stay on the payroll by stealing computer files and other sensitive material.

The CIA had suspected the presence of a mole in the agency since 1986, when the first two of the Soviet agents Ames betrayed were executed. Suspicions grew with every execution and disappearance of Soviet agents in the late 1980s. The CIA was aware of Ames's extravagant spending as early as 1990. Ames passed inquiry lie-detector

tests in 1986 and 1991. However, In 1993, a joint investigation between the Federal Bureau of Investigation and the CIA narrowed a list of 200 suspects down to fewer than 40, and then down to Aldrich Ames. In May, 1993, they launched project "Nightmover," a criminal investigation under the FBI's jurisdiction charged with gathering evidence against Ames.

Compiling enough evidence to arrest Ames and his wife on conspiracy charges took nearly a year. Over one hundred FBI agents, some of them elite members of the Special Services Group, tapped Ames's phone wires, rooted through his garbage, planted a wire in his Jaguar, installed a video camera across from his house, shadowed him disguised as trash collectors and lawn maintenance workers, and kept his home under nearly constant surveillance.

The big break in the case occurred in early September, 1993. Ames was overheard talking on his cell phone with his wife. The conversation included details about a pending deal with Russian agents. A few days later, he was seen near what was assumed to be the signal or dead drop site used by Ames and his Russian contacts. On September 15, the FBI found a note in Ames's garbage can indicating he was arranging a meeting for October. The FBI then obtained a warrant to enter Ames's house. While Ames and his family were away for a weekend in early October, the FBI searched his home, finding in his personal computer detailed information about drop sites and meeting places along with files of classified CIA information Ames had no business taking home. They followed him to Bogota where he was to meet with his handler, Yuri Karetkin, but failed to catch him in the act. Ames returned home \$125,000 richer.

Nothing happened for four months. Ames appeared to be laying low. Finally, after detecting an unusual number of Russian intelligence officers lurking around Ames's neighborhood, the FBI became worried that the Russians had guessed Ames was under investigation. Ames was scheduled to go to Moscow and the FBI feared he might defect. The FBI decided to act, even though they had not been able to catch Ames actually meeting with his Russian handler. Aldrich and Rosario Ames were arrested on February 21, 1994, and charged with espionage. To prevent them from fleeing the country, the couple were held without bail.

The Ames espionage case, called a "calamity" by the Senate Intelligence Committee, remains one of the most remarkable cases of double-dealing in the history of the United States. The case is remarkable not only because Ames made so much money selling CIA secrets and because of the huge amount of information he sold, allegedly compromising over a hundred covert operations, but also because Ames remained undetected for so long. The case prompted an investigation by the Senate into counterintelligence procedures at the CIA and calls from Congress and the public for sweeping reform of the agency.

Following the Senate Intelligence Committee's report, some minor reforms were instituted to guard against the possibility of another security breach.

Ames was sentenced to life in prison without the possibility of parole. To gain leniency for his wife, Ames plead guilty to all charges levied against him.

#### ■ FURTHER READING:

##### BOOKS:

Nash, Jay Robert. *Spies: A Narrative Encyclopedia of Dirty Deeds and Double Dealing from Biblical Times to Today*. M.Evans, 1997.

##### SEE ALSO

*CIA (United States Central Intelligence Agency)*  
*KGB (Komitet Gosudarstvennoi Bezopasnosti, USSR Committee of State Security)*  
*Russia, Intelligence and Security*  
*Hanssen (Robert) Espionage Case*

## Anthrax

#### ■ BRIAN HOYLE

In the 1990s, the use of biological weapons by terrorists became a serious threat to the security of countries around

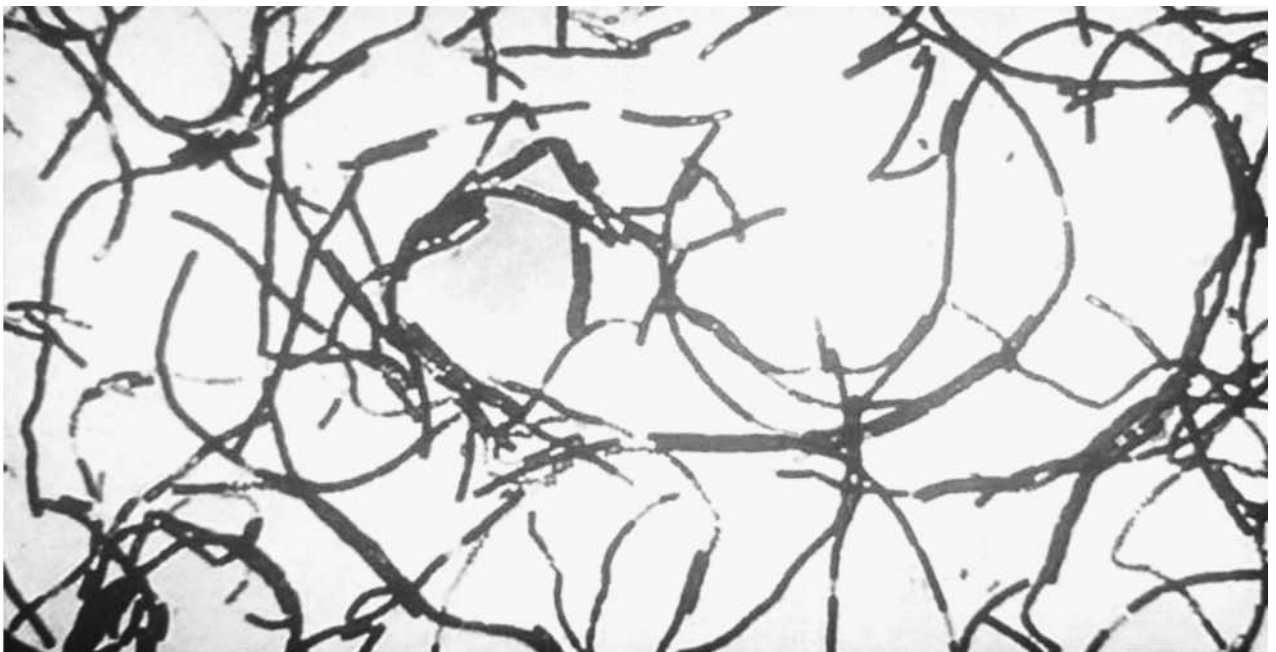
the globe, and the United States in particular. During the Gulf War of 1990 to 1991, and in subsequent United Nations inspection efforts, the government of Iraq's development of advanced anthrax based bioweapons was revealed.

Although the incidents have not been directly linked, following the September 11, 2001 terrorist attacks on the World Trade Center buildings in New York City and the Pentagon in Washington, D.C., anthrax was used as a bioterrorist weapon. Letters containing a powdered form of *Bacillus anthracis*, the bacteria that causes anthrax, were mailed to representatives of government and the media, among others. Multiple attacks eventually killed five people.

Anthrax refers to a disease that is caused by the bacterium *Bacillus anthracis*. The bacterium can enter the body via a wound in the skin (cutaneous anthrax), via contaminated food or liquid (gastrointestinal anthrax), or can be inhaled (inhalation anthrax). The latter in particular can cause a very serious, even lethal, infection.

The disease has been present throughout recorded history. Its use as a weapon stretches back centuries. Hundreds of years ago, bodies of anthrax victims were dumped into wells, or were catapulted into enemy encampments. Development of anthrax-based weapons was pursued by various governments in World Wars I and II, including those of the United States, Canada, and Britain.

Humans naturally acquire anthrax from exposure to livestock such as sheep or cattle or wild animals. The animals are reservoirs of the anthrax bacterium.



A microscopic view of the anthrax bacteria is seen in this photo from the U.S. Army Medical Research and Development Command at Ft. Detrick, Maryland. AP/WIDE WORLD PHOTOS.

While all three types of anthrax infections are potentially serious, prompt treatment usually cures the cutaneous form. Even with prompt treatment, the gastrointestinal form is lethal in 25%–75% of those who become infected. The inhaled version of anthrax is almost always lethal.

When *Bacillus anthracis* is actively growing and dividing, it exists as a large “vegetative” cell. But, when the environment is threatening, the bacterium can form a spore and becoming dormant. The spore form can be easily inhaled. Only 8,000 spores, hardly enough to cover a snowflake, are sufficient to cause the inhalation form of anthrax when the spores resuscitate and begin growth in the lungs.

The growing *Bacillus anthracis* cells have several characteristics that make them so infectious. First, the formation of a capsule around the bacterium can mask the surface from recognition by the body’s immune system. The body can be less likely to mount an immune response to the invading bacteria. Also, the capsule helps fend off antibodies and immune cells that do respond. This protection can allow the organism to multiply to large numbers.

The capsule also contains a protein that protects the bacterium. This “protective antigen” dissolves other protein molecules that form part of the outer coating of host cells. This allows the bacterium to evade the host’s immune response by burrowing inside host cells such as the epithelial cells that line the lung.

A toxic component called lethal factor actively destroys the host’s immune cells. Finally, another toxic factor called the edema factor (edema is the build up of fluid at the site of infection) disables a host molecule called calmodulin. Calmodulin regulates many chemical reactions in the body.

With the various toxic factors, *Bacillus anthracis* is able to overcome the attempts of the host to deal with the infection. Bacterial toxins enter the bloodstream and circulate throughout the body. The destruction of blood cells and tissues can be lethal.

The early symptoms of anthrax infections are similar to other, less serious infections, such as the flu. By the time the diagnosis is made, the infection can be too advanced to treat. This can make the recognition of a deliberate anthrax attack difficult to recognize until large numbers of casualties have resulted. While the bacteria can be killed by antibiotics, in particular an antibiotic called ciprofloxacin (cipro), the antibiotic needs to be administered early in an infection.

The ease by which anthrax can be transported (i.e., via the mail) has made anthrax a weapon of frightening severity.

A vaccine for anthrax does exist, although the possibility of serious side effects has limited its use to only those at high risk for infection (i.e., soldiers, workers in meat processing plants, anthrax researchers). Vaccine

researchers are exploring the possibility that the edema factor and the capsule could be exploited as targets of vaccines. The idea is that the vaccines would stop the bacteria from getting into host cells. This would make it easier for the immune response to kill the invading bacteria.

#### ■ FURTHER READING:

##### BOOKS:

Heyman, D. A., J. Achterberg, and J. Laszlo. *Lessons from the Anthrax Attacks: Implications for U.S. Bioterrorism Preparedness: A Report on a National Forum on Biodefense*. Washington, DC: Center for Strategic and International Studies, 2002.

Koehler, T. M. *Anthrax*. Berlin: Springer Verlag, 2002.

##### PERIODICALS:

Jernigan, J. A., D. S. Stevens, D. A. Ashford, et al. “Bioterrorism-Related Inhalational Anthrax: The First 10 Cases Reported in the United States.” *Emerging Infectious Diseases* no. 7 (2001).

##### ELECTRONIC:

Centers for Disease Control and Prevention. “Anthrax.” Division of Bacterial and Mycotic Diseases. October 30, 2001. <[http://www.cdc.gov/ncidod/dbmd/diseaseinfo/anthrax\\_t.htm](http://www.cdc.gov/ncidod/dbmd/diseaseinfo/anthrax_t.htm)>(9 December 2002).

##### SEE ALSO

*Anthrax, Terrorist Use as a Biological Weapon*

*Anthrax Vaccine*

*Anthrax Weaponization*

*Antibiotics*

*Biological Weapons, Genetic Identification*

*Infectious Disease, Threats to Security*

*USAMRIID (United States Army Medical Research Institute of Infectious Diseases)*

## ..... Anthrax, Terrorist Use as a Biological Weapon .....

#### ■ BRIAN HOYLE

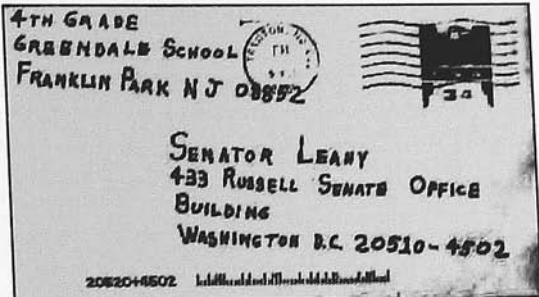
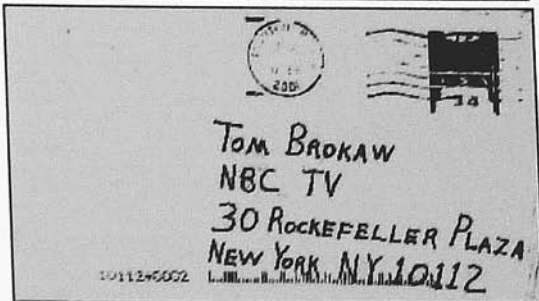
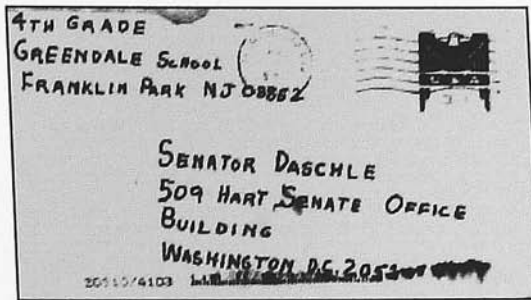
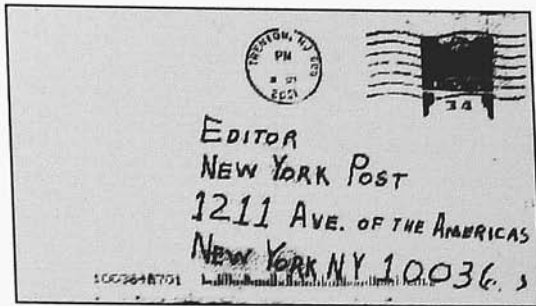
During the past two decades, the potential use of biological weapons by terrorist groups has received a great deal of attention, particularly in the United States. The existence of an anthrax bioweapon development campaign by the government of Iraq was revealed during the Persian Gulf War from 1990 to 1991. Then, in the aftermath of the September 11, 2001 terrorist attacks on the World Trade Center buildings in New York City and the Pentagon in Washington, DC, letters containing a powdered form of *Bacillus anthracis*, the bacteria that causes anthrax, were mailed to government representatives, members of the news media, and others in the United States. The anthrax-laced powder inside the letters was aerosolized (i.e., the



# REWARD UP TO \$2,500,000



For information leading to the arrest and conviction of the individual(s) responsible for the mailing of letters containing anthrax to the New York Post, Tom Brokaw at NBC, Senator Tom Daschle and Senator Patrick Leahy:



## AS A RESULT OF EXPOSURE TO ANTHRAX, FIVE (5) PEOPLE HAVE DIED.

The person responsible for these deaths...

- Likely has a scientific background/work history which may include a specific familiarity with anthrax
- Has a level of comfort in and around the Trenton, NJ area due to present or prior association

Anyone having information, contact **America's Most Wanted** at  
**1-800-CRIME TV** or the **FBI** via e-mail at [amerithrax@fbi.gov](mailto:amerithrax@fbi.gov)

All information will be held in strict confidence. Reward payment will be made in accordance with the conditions of Postal Service Reward Notice 296, dated February 2000. Source of reward funds: US Postal Service and FBI \$2,000,000; ADVO, Inc. \$500,000.



The FBI and the U.S. Postal Service released this reward flyer for information leading to the arrest and conviction of the individuals responsible for mailing anthrax-tainted letters in 2001 to members of Congress and the media. AP/WIDE WORLD PHOTOS.

spores became airborne) when the letters were opened, and in a few cases were inhaled. The death of a Florida man was the first case of an inhalational anthrax death in the United States since 1978 and as of June 2002, more than 20 cases and five deaths were attributed to the terrorist attacks.

Although anthrax is a relatively new weapon in the hands of modern potential bioterrorists, the threat of death from the inhalation of spores has been part of human history since antiquity. Some scholars argue that anthrax is the sooty "morain" in the Bible's Book of Exodus, and is likely the "burning wind of plague" that begins Homer's *Iliad*.

As well, the use of microorganisms such as the anthrax bacteria as weapons is not new. In ancient military campaigns, diseased bodies (including those who died of anthrax) were used to poison wells and were catapulted into cities under siege. Research into the military use of anthrax was carried out during World War I by combatants on all sides of the conflict, and by World War II, anthrax research was actively underway. For example, Allied efforts in Canada, the United States, and Britain to develop anthrax-based weapons included the production of five million anthrax "cakes," designed to be dropped on Germany to infect wells and contaminate the food chain. The weapons were never used.

Only within the past several decades, however, have biological weapons, including anthrax, been added to the arsenal of terrorists. For example, the Japanese cult Aum Shinrikyo (which released Sarin gas into the Tokyo subway system in 1995, killing 12 people and hospitalizing 5,000) was developing anthrax-based weapons. Indeed, the group had released crude anthrax preparations in Tokyo on at least eight separate occasions in 1993. These incidents constituted the first use of anthrax as a weapon against a civilian population. In addition, state-sanctioned terrorism by the government of Iraq has also involved the production of anthrax bioweapons, and Western intelligence sources openly insist that Iraq—and or terrorist groups operating with Iraq's assistance—continued to develop biological weapons, including anthrax based weapons. Finally, during the terrorist attacks of the United States in the latter part of 2001, the use of anthrax by a terrorist or terrorists (as of July, 2003, yet unidentified) pointed out how easily the lethal agent could be delivered.

This ease of delivery of anthrax is one feature that has made the bacterium an attractive weapon for terrorists. Scenarios developed by United States government agencies have shown that even a small crop dusting plane carrying only a hundred kilograms of anthrax spores flying over a city could deliver a potentially fatal dose to up to three million people in only a few hours. Although variations in weather patterns and concentration variables would substantially reduce the number of expected actual deaths, such an attack could still result in the deaths of thousands of victims and result in a devastating attack on the medical and economic infrastructure of the city attacked. In a less sophisticated effort, spores could simply

be released into air intake vents or left in places like a subway tunnel, to be dispersed in the air over a much smaller area.

Another feature of anthrax that has led to its exploitation by terrorists is the physiology of the bacterium. *Bacillus anthracis* can live as a "vegetative cell," growing and dividing in a rapid and cyclical fashion. The bacterium can also form a metabolically near-dormant form known as a spore. An individual spore is much smaller and lighter than the growing bacterium. The spores can drift on air currents, to be inhaled into the lungs. Once in the lungs, the spores can resuscitate into an actively growing and dividing bacterium. The infections that are collectively termed anthrax can result. Although millions of spores can be released from a few grams (fractions of an ounce) of *Bacillus anthracis*, only about 5,000 to 8,000 spores are sufficient to cause the lung infection when they are inhaled. If left untreated or not promptly treated with the proper antibiotics (such as Cipro), the lung infection is almost always fatal. Non-inhalation contact with *Bacillus anthracis* can result in cutaneous anthrax—a condition more treatable with conventional antibiotic therapy.

An often-overlooked aspect of the use of anthrax as a terrorist weapon is the economic hardship that the dispersal of a small amount of the spores would exact. A report from the Centers for Disease Control and Prevention, entitled *The Economic Impact of a Bioterrorist Attack*, estimated the costs of dealing with an anthrax incident at a minimum of U.S. \$26 billion per 100,000 people. In just a few months in 2001 alone, a flurry of anthrax incidents, most of which turned out to be hoaxes, cost the United States government millions of dollars.

**Biotechnology and anthrax.** The choice of anthrax as a weapon used by terrorists reflects the growing awareness of the power of biological research and biotechnology among the general community. The ability to grow and disperse infectious microorganisms was once restricted to specialists. However, the explosion of biotechnology in the 1980s and 1990s demonstrated that the many basic microbiological techniques are fairly simple and attainable. Experts in microbiology testifying before the U.S. Congress estimated that crude weapons could be developed with approximately \$10,000 worth of equipment. A laboratory sufficient to grow and harvest the bacteria and to dry down the material to powdered form could fit into the average sized household basement. The more highly trained the terrorist, the more effective weapons could be expected to be produced.

Even though *Bacillus anthracis* could be grown in such a makeshift laboratory, the preparation of the spores and the drying of the spores into a powder is not a trivial task. For example, even after a decade of dedicated effort, United Nations inspectors who toured Iraq bioweapons facilities after the Gulf War found that Iraq had only managed to develop crude anthrax preparations. Still, the Iraqi

bioweapons program managed to produce 8,500 liters of concentrated anthrax.

Despite the technical challenges, the production of anthrax spores in quantities great enough to cause a huge loss of life is not beyond the capability of a small group of equipped and funded terrorists. The small size and nondescript nature of a bioweapons facility could make detection of such a lab very difficult. Accordingly, the terrorist potential of anthrax will remain a threat for the foreseeable future.

## ■ FURTHER READING:

### BOOKS:

Heyman, D. A., J. Achterberg, and J. Laszlo. *Lessons from the Anthrax Attacks: Implications for U.S. Bioterrorism Preparedness: A Report on a National Forum on Biodefense*. Washington, DC: Center for Strategic and International Studies, 2002.

Inglesby, Thomas V. "Bioterrorist Threats: What the Infectious Disease Community Should Know about Anthrax and Plague", in: *Emerging Infections 5* Washington, DC: American Society for Microbiology Press, 2001.

Koehler, T. M. *Anthrax*. Berlin: Springer Verlag, 2002.

### ELECTRONIC:

University of California at Los Angeles. "Anthrax as a Weapon." College of Letters and Science. February, 2002. <<http://www.college.ucla.edu/webproject/micro12/m12webnotes/anthraxweapon.html>> (29 December 2002).

### SEE ALSO

*Anthrax Vaccine*  
*Bacterial Biology*  
*Biological Warfare*  
*Bioterrorism, Protective Measures*

---

## Anthrax Vaccine

---

### ■ BRIAN HOYLE

Anthrax is an infection that is caused by the bacterium *Bacillus anthracis*.

Several different types of anthrax infection can be caused by the bacterium. Entry of bacteria through a skin wound can produce a skin infection known as cutaneous anthrax. Microorganisms can also contaminate food or water. Ingestion of the contaminated food or water produces gastrointestinal anthrax. The most serious type of anthrax results from the inhalation of the spore form of the bacterium. Inhalation anthrax has a high mortality rate.

In the 1990s, United States military personnel in the Persian Gulf region faced the possibility of retaliatory strikes using biological weapons, in particular anthrax.

Domestically, the use of *Bacillus anthracis* spores by terrorists is a reality. Although not directly related by evidence to the September 11, 2001, terrorist attacks on the World Trade Center and Pentagon in the United States, letters containing powdered anthrax bacteria and spores were sent to a number of politicians, media personalities, and U.S. citizens. Even more ominously, the terrorists responsible for the September 11 attacks had attempted to procure a small crop dusting aircraft. Such an aircraft could potentially disperse several hundred kilograms of anthrax spores upwind of a major urban center in only a few hours. One scenario developed by scientists for Washington, D.C. indicated that up to three million people could be sickened or killed by such an attack.

For some years, military personnel and others at risk for anthrax exposure (i.e., researchers and those handling animals) have received an anthrax vaccine. For example, U.S. military personnel were vaccinated in 1990, during the Gulf War, and again prior to another response in that region in 1998.

The increasing risk and incidence of anthrax exposure, however, have made the development of different and safer anthrax vaccines a priority. The use of anthrax against civilians, and the ominous scenarios of anthrax spores released in the ventilation systems of office buildings and over large urban centers, have created the possibility that millions of people would potentially require vaccination. As well, large stockpiles of anthrax vaccine (as well as antibiotics) would be required, in anticipation of future outbreaks.

**Current anthrax vaccine.** The anthrax vaccine now in use dates back to the time of Louis Pasteur, in the mid-nineteenth century. Pasteur noted that the injection of animals with an attenuated type of *Bacillus anthracis* protected the animals from contracting anthrax. An attenuated strain of bacteria is one that can be capable of growth, but which does not cause disease. The body's immune system will react to the bacteria, and produce antibodies that will protect the animal or person from future exposure to the disease-causing bacteria. A modification of this attenuated vaccine developed in the late 1930s still serves as the anthrax vaccine given to animals.

In the late nineteenth century, the use of live bacteria as vaccines was still too dangerous for humans. In the early years of the twentieth century, researchers began exploring the use of components of the anthrax bacterium as a protective measure. In 1954, a product was developed that consisted of soluble material called protective antigen, which is released by *Bacillus anthracis*, and which can be precipitated out of solution—along with two other cell components called the lethal factor and the edema factor—by the use of aluminum potassium sulfate (alum). Filtering the suspension captures the antigenic compounds.

By 1960, the selection of a strain of *Bacillus anthracis* that produced more of the protective antigen, the use of





A technician works in a clean room filling anthrax vaccine vials at a Spokane, Washington, laboratory in 2002. AP/WIDE WORLD PHOTOS.

growth media that was free of protein (that could also stimulate an immune reaction), and the use of aluminum hydroxide instead of alum had produced a superior vaccine. The improved product, anthrax vaccine adsorbed (AVA), was approved for use in the United States in 1965. AVA remains the only licensed vaccine in the United States as of early 2003.

**Protective antigen, lethal factor, and edema factor.** The protective antigen is a protein that can insert into the membrane of a host cell to create a hole, or pore, through the membrane. The pore then functions as a portal to allow the other two components to get inside of the host cell.

The lethal factor is a type of enzyme classified as a zinc protease. The enzyme attacks and breaks host proteins into smaller and nonfunctional pieces. Destroying

host cell proteins is lethal to the host cell, hence the factor's name.

Edema factor is a toxin. The destruction of the host cells allows this toxin to enter the bloodstream, where it can kill cells of the immune system. Disabling the host's immune response allows the bacteria and the toxin to spread throughout the body.

**Side effects of the anthrax vaccine.** Like some other vaccines, AVA can cause side effects, which can, in rare instances, be life threatening or fatal. Data regarding adverse events are available from the Vaccine Event Reporting System (a U.S. vaccine safety surveillance program that is under the direction of the Food and Drug Administration and the Centers for Disease Control and Prevention). From January 1, 1990 through August 31, 2000, 1,859,000 doses of anthrax vaccine were administered in

the United States. The number of adverse events was 1,544 (e.g. sensitivity at injection site, headache, muscle ache) with 76 of these being serious (e.g., heart failure, blood infection). Other than reaction at the site of injection, it is still not clear whether the other maladies were directly due to the vaccine. Nonetheless, the number of adverse reactions were small.

Echoing this data, a report released in March 2002 by the U.S. National Academy of Sciences Institute of Medicine concluded that AVA is "acceptably safe." However, the report noted the lack of data on the long-term effects of the vaccine.

Studies conducted by the Department of Defense on vaccinated military personnel found that most adverse events were minor, were localized to the site of injection, and cleared up within a few days.

The involvement of anthrax vaccine to the development of a multi-symptom debilitating syndrome reported in military personnel deployed in the Persian Gulf conflicts ("Gulf War Syndrome") was investigated by the Centers for Disease Control and Prevention. No scientific evidence of an association was found. However, studies conducted on Canadian and British soldiers stationed in the Gulf and in Bosnia (where anthrax deployment was also a threat) were not as conclusive.

**Limitations of the anthrax vaccine.** While the risks posed by AVA may not be pronounced, the vaccine is problematic from the standpoints of supply and quality of the product.

In addition to aluminum, the vaccine contains benzethonium chloride as a preservative and formaldehyde to keep the vaccine mixture stable upon storage. Despite regulatory examinations that have confirmed the safety of the vaccine, there continues to be debate as to the possible long-term harm from the presence of these chemicals.

Another problem concerns the frequency of vaccination that is required to establish immunity. Primary vaccination requires three injections at 0, 2, and 4 weeks, followed by three booster injections at 6, 12, and 18 months. To maintain the immunity, annual injections are recommended.

Such a frequent regimen of injections is inconvenient and requires almost two years to establish peak protection. The vaccine is not designed to confer rapid immunity.

The nature of the vaccine's preparation—collection of material extruded by the bacteria—makes the vaccine crude in terms of its exact composition and proportion of the various components. This unpredictability, and the scarcity of the vaccine have limited the wide-spread availability of AVA.

The vaccine is currently manufactured at a single facility in the U.S., and only in sufficient quantity for use by those at risk of infection, such as combat personnel and researchers.

## ■ FURTHER READING:

### PERIODICALS:

Advisory Committee on Immunization Practices. "Recommendations of the Advisory Committee on Immunization Practices: Use of Anthrax Vaccine in the United States." *Morbidity and Mortality Weekly Report* no. 49 (2000): 1–20.

Bradley, K. A., J. Mogridge, M. Mourey, et al. "Identification of the Cellular Receptor for Anthrax Toxin." *Nature* no. 414 (2001): 225–229.

Friedlander, A. M. "Tackling Anthrax." *Nature* no. 414 (2001): 160–161.

Joellenbeck, L. M., L. L. Zwanziger, J. S. Durch, et al. *The Anthrax Vaccine: Is It Safe? Does It Work?* Washington, DC: National Academies Press, 2002.

### SEE ALSO

*Biological Warfare*  
*Microbiology: Applications to Espionage, Intelligence and Security*  
*Toxins*

---

## Anthrax Weaponization

---

### ■ BRIAN HOYLE

The lethality of inhalation anthrax, combined with the ability of the lethal payload to be delivered in the spore form, has made anthrax an attractive candidate for weaponization. In addition, a vaccine to anthrax does exist, but is not yet widely available. Thus, troops can be vaccinated against the disease while the general population of the enemy remains unprotected. Many of these characteristics that make anthrax a desirable military weapon also make the disease a desirable weapon of the terrorist.

As of 2003, intelligence sources indicate that at least 17 nations around the globe have offensive biological weapons programs. How many of these nations are pursuing anthrax weaponization is unknown. The government of Iraq, however, admitted in 1995 to producing over 8,000 liters of concentrated anthrax as part of the nation's biological weapons program. Additionally, only a few generations ago, nations such as Britain and the United States actively engaged in anthrax weaponization programs.

Anthrax is a disease that is caused by the bacterium *Bacillus anthracis*. The bacterium lives naturally in grazing animals such as cattle and sheep. Depending on the route of entry of the bacterium into the human body, anthrax infection can occur in the intestinal tract, the skin, and, most seriously, in the lungs. The latter form, which is called pulmonary or inhalation anthrax, progresses swiftly and is lethal in over 50%. Early detection of the infection,



Members of an EPA and United States Coast Guard cleanup crew prepare to enter the American Media Inc. office building in Boca Raton, Florida, where at least two people contracted anthrax through a deliberately contaminated letter mailed to the facility in October, 2001. AP/WIDE WORLD PHOTOS.

combined with the use of antibiotic and supportive therapies offer the best chance of survival once an inhalation anthrax infection has been established.

A major factor that contributes to the spread of anthrax is the ability of the bacterium to form a spore. The spore is a tough shell that houses the genetic material of the microbe, and can preserve this material almost indefinitely through harsh environmental conditions that would kill the growing bacteria. When conditions become more hospitable—as when the spores are breathed into the

warm and moist environment of the lungs—the spores “germinate” and bacterial growth resumes.

Most biological warfare experts concur that the manufacture of sufficient quantities of anthrax spores to permit an aerial assault or to form the payload of missiles requires manufacturing facilities and skilled personnel, and is a formidable challenge. Nonetheless, given time, funding and desire, an organization can muster the necessary resources. For example, the terrorist group Aum Shinrikyo, which was responsible for the release of Sarin gas in a Tokyo, Japan, subway station in 1995, also released spores

of *Bacillus anthracis* and *Clostridium botulinum* (the bacterium that causes botulism) throughout Tokyo on at least eight occasions.

The dispersal of anthrax via a crop dusting plane or a balloon is the most likely scenario for the mass exposure of a population. More traditional methods use missiles to deliver the payload of explosives. However, the heat that develops in a missile during its passage to the target, particularly as it re-enters the atmosphere, could kill even anthrax spores.

The most popular anthrax weapon to date has been the dried form of the bacterial spores. The powdery material becomes dispersed in the air very easily. For example, opening a letter can disperse the powder and cause spores to be inhaled.

In contrast, the process of manufacturing the spore powder is technically complex. When anthrax bacteria for spores and the spores are harvested, they form a sticky paste with the consistency of peanut butter. When this paste is dried, the result is a hard block of material. The block can be ground into a powder. But the spores will tend to have a surface charge and so will tend to clump together. The clumping can be overcome by coating the spores with chemicals such as silica or alumina clay. The Iraqi program utilized a clay preparation called bentonite.

For the spores to be inhaled deep into the lungs, each spore needs to be on the order of one to five micrometers in diameter. Anything smaller than this will behave as a gas, and so will be exhaled, while larger particles such as the clumps of spores will become stuck in the upper respiratory tract, where it is more difficult to establish the disease. Preparation of a spore powder where all the particles are the requisite size is not, in terms of difficulty, a trivial task. Nonetheless, the success of the anthrax terrorist attacks in the U.S. in 2001 shows that it is possible.

Studies on Gruinard Island—an island off the coast of Scotland where Britain conducted tests of anthrax spore delivery systems during World War II—has recovered spores that can germinate into disease causing bacteria even decades later. Thus, even an inefficient application of anthrax spores may leave a residual that will be capable of infecting people for long after the attack.

#### ■ FURTHER READING:

##### BOOKS:

Heyman, D.A., J. Achterberg, and J. Laszlo. *Lessons from the Anthrax Attacks: Implications for U.S. Bioterrorism Preparedness: A Report on a National Forum on Biodefense*. Washington, DC: Center for Strategic and International Studies, 2002.

##### ELECTRONIC:

University of California at Los Angeles. "Anthrax as a Weapon." College of Letters and Science. February,

2002. <<http://www.college.ucla.edu/webproject/micro12/m12webnotes/anthraxweapon.html>> (29 December 2002).

#### SEE ALSO

*Biological Warfare*  
*Coordinator for Counterterrorism, United States Office*  
*Infectious Disease, Threats to Security*

---

## Antiballistic Missile Treaty

---

■ LARRY GILMAN

The Antiballistic Missile (ABM) Treaty was signed by the United States and the Soviet Union (U.S.S.R.) in 1972. The treaty was one of two treaties produced by the first series of Strategic Arms Limitation Talks (SALT I) between the two countries; the other was an interim agreement limiting offensive nuclear weapons. The ABM treaty strictly limited the deployment—by both sides—of interceptor missiles, missile launchers, radars, and other devices designed to destroy ballistic missiles or their components in flight. In the original version, each nation was permitted to retain a limited number of ABM radars and no more than 100 ABM interceptor missiles at each of two circular sites 186 miles (300 km) in diameter, one centered on the nation's capital and the other on a cluster of ballistic-missile launch sites. A 1974 amendment reduced the number of permitted ABM sites to one per side and further bound both countries to not deploy ABM systems outside their own territory (e.g., at sea or on the territory of allies). In 1975, the U.S. dismantled its sole ABM system, SAFE-GUARD; the U.S.S.R. (and, later, the Russian Federation) retained a single ABM system centered on Moscow. In 1997, further minor revisions were agreed upon, but never ratified by the U.S. The U.S. withdrew from the ABM treaty in July, 2002, and it is no longer binding on any country.

In the U.S., critics urged withdrawal from the ABM treaty soon after it was signed. They argued that it was ridiculous to prevent nuclear war by limiting defense against the primary means for delivering nuclear weapons to their targets. The Reagan administration, for example (1980–1988) sought to deploy an ambitious missile-defense system ("Star Wars") that would have required abrogation of the ABM treaty. However, supporters of the ABM treaty defended it successfully throughout the 1980s and 1990s based primarily upon the concepts of mutual deterrence, mutual destruction, and first-strike capability.

Since the 1950s, the U.S. and the Soviet Union (U.S.S.R.) possessed enough nuclear warheads mounted on ballistic missiles (and additional thousands on other delivery systems, such as bombers) to destroy each other many times over. Aggression by each side was, in theory, deterred by fear of the other side's weapons; if either side attacked, both attacker and attacked would be destroyed.



With his national security team assembled in the Rose Garden at the White House, President Bush, center, announces that the United States will withdraw from the 1972 Anti-ballistic Missile Treaty in 2002, paving the way for the development of a defensive anti-ballistic missile technology program. AP/WIDE WORLD PHOTOS.

This policy—often termed Mutually Assured Destruction—was unstable to the extent that a “first strike” by one side was able (or was perceived as being able) to destroy the other side’s missiles in their silos, eliminating most of that country’s ability to retaliate. If such a strike were successful, the country to strike first might prevail. Building defenses against ballistic missiles, most arms-control experts assumed, would make this situation even more unstable for several reasons. First, it is impossible to build a system of antiballistic-missile weapons that can reliably protect most of the civilian population of any nation from a determined nuclear attack. (2) A partially effective shield, however, might serve to protect a nuclear aggressor from the effects of a weak counterattack. (3) Possession of such a partial defensive system would, therefore, make a first strike more attractive to the nation possessing it. (4) Finally, if one side built such a partial system, the other, knowing that a first strike had become more attractive to side possessing the partial ABM system, would have even more incentive to strike first itself (against the enemy’s ABM system as well as its offensive nuclear weapons), and place itself on hair-trigger alert against attack, making accidental nuclear war more likely. The ABM treaty was designed, signed, and ratified by the U.S. and U.S.S.R. in order to prevent destabilization of this type.

The Reagan administration was prevented from developing a Star Wars system by domestic political resistance centered on the ABM treaty and on skepticism about the technical feasibility of the Stars Wars concept itself. However, the project has been funded by all succeeding administrations, and has now been fully revived under President George W. Bush. In December 2001, the United States gave six months’ notice of its intent to withdraw

from the ABM treaty, as provided for by the terms of the treaty itself. The U.S. officially withdrew from the treaty in July, 2002. A few days later, work began on a U.S. missile shield, with ground-breaking ceremonies at Fort Greeley, Alaska for a test-bed ABM system consisting of six interceptor missiles.

China, which at present has only about 20 intercontinental-range, land-based ballistic missiles, has stated that it is able to build offensive systems capable of overwhelming any ABM system deployed by the United States.

#### ■ FURTHER READING:

##### BOOKS:

Alves, Péricles Gasparini. *Prevention of an Arms Race in Outer Space*. New York: United Nations Institute for Disarmament Research. 1991.

##### ELECTRONIC:

Stoullig, Jean-Michel. “ABM Treaty Ends, U.S. Open to Experiment on Missile Defense.” *Agence France-Presse* (in SpaceDaily.com). June 13, 2002. <<http://www.spacedaily.com/news/bmdo-021.html>> (December 9, 2002).

“Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Limitation of Anti-Ballistic Missile Systems, 944 U.N.T.S. 13.” Nuclear Age Peace Foundation. 2002. <<http://www.nuclearfiles.org/docs/1972/720526-abm.html>> (December 9, 2002).

##### SEE ALSO

*Ballistic Missile Defense Organization, United States Ballistic Missiles*

## Antibiotics

■ BRIAN HOYLE

The security and stability of a country depends in part on the health of its citizens. One of the factors that influence the health of people is infectious disease (a disease that can be spread from person to person or from another living being to a human). A variety of infectious diseases are caused by bacteria.

Some bacterial infections can be treated using compounds that are collectively known as antibiotics. Antibiotics can be naturally produced. For example, the first antibiotic discovered (penicillin; discovered in 1928 by Sir Alexander Fleming) is produced by a species of a mold microorganism. There are a variety of different naturally produced antibiotics, while many other antibiotics have been chemically produced. Finally, antibiotics act only on bacteria and are not effective against viruses.

Prior to the discovery of penicillin there were few effective treatments to battle or prevent bacterial infections. Pneumonia, tuberculosis, and typhoid fever were virtually untreatable. And, in those persons whose immune system was not functioning properly, even normally minor bacterial infections could prove to be life-threatening.

In nature, antibiotics help protect a bacteria or eukaryotic cell (i.e., plant cell) from invading bacteria. In the laboratory, this is evident as the inhibition of growth of bacteria in the presence of the antibiotic-producing species. This screening can be automated so that thousands of samples can be processed each day.

The chemical synthesis of antibiotics is now very sophisticated. The antibiotic can be tailored to affect a specific target on the bacterial cell. Three-dimensional modeling of the bacterial surface and protein molecules is an important aid to antibiotic design.

Penicillin is in a class of antibiotics called beta-lactam antibiotics. The name refers to the chemical ring that is part of the molecule. Other classes of antibiotics include the tetracyclines, aminoglycosides, rifamycins, quinolones, and sulphonamides. The action of these antibiotics is varied. The targets of the antibiotics are different. Some antibiotics disrupt and weaken the cell wall of bacteria (i.e., beta-lactam antibiotics), which causes the bacteria to rupture and die. Other antibiotics disrupt enzymes that are vital for bacterial survival (aminoglycoside antibiotics). Still other antibiotics target genetic material and stop the replication of deoxyribonucleic acid (DNA) (i.e., quinolone antibiotics).

Antibiotics can also vary in the bacteria they affect. Some antibiotics kill only a few related types of bacteria and are referred to as narrow-spectrum antibiotics. Other antibiotics such as penicillin kill a variety of different bacteria. These are the broad-spectrum antibiotics.

Following the discovery of penicillin, many different naturally occurring antibiotics were discovered and still many others were synthesized. They were extremely successful in reducing many infectious diseases. Indeed, in the 1970s the prevailing view was that infectious diseases were a thing of the past. However, beginning in the 1970s and continuing to the present day, resistance to antibiotics is developing.

As of 2002, the problem of antibiotic resistance is so severe that many physicians and security analysts think that the twenty-first century will initiate the "post antibiotic era." In other words, the use of antibiotics to control infectious bacterial disease will no longer be an effective strategy.

Resistance to a specific antibiotic or a class of antibiotics can develop when an antibiotic is overused or misused. If an antibiotic is used properly to treat an infection, then all the infectious bacteria should be killed directly, or weakened such that the host's immune response will kill them. However, if the antibiotic concentration is too low, the bacteria may be weakened but not killed. The same thing can happen if antibiotic therapy is stopped too soon. The surviving bacteria may have acquired resistance, which can be genetically transferred to subsequent generations of bacteria. For example, many strains of *Mycobacterium tuberculosis*, the bacterium that causes tuberculosis, are resistant to one or more of the antibiotics used to treat the lung infection. Some strains of *Staphylococcus aureus* that can cause boils, pneumonia, or bloodstream infections, are resistant to most (and with one strain, all) antibiotics.

The increasing antibiotic resistance of bacteria, and the resulting increase in infectious diseases, is a security risk. Disease can decimate the population. The misery and economic hardship that results can cause political instability. In underdeveloped countries, this instability can lead to anger directed at developed countries such as the United States. Even in developed countries, the increasing numbers of people needing hospitalization and medical care can strain the health care system.

The availability of antibiotics to combat bacterial epidemics has always been challenging. The appearance and rapid increase in an infection can tax the ability of a healthcare system to respond with medicines including the appropriate antibiotics.

The threat of biological warfare, such as the aerial distribution of *Bacillus anthracis*, the agent of anthrax, has made the provision of large quantities of antibiotics a priority for the United States and other nations. Plants that manufacture antibiotics are designed with sterility of manufacture in mind, not security. Disabling an antibiotic manufacturing facility would be a crippling blow to any potential biowarfare response.

Even if a large supply of a particular antibiotic were available, the emergency response would be challenging, as the antibiotic would need to be distributed to many

people (i.e., millions in the event of an aerial release of the anthrax bacterium) within hours.

#### ■ FURTHER READING:

##### PERIODICALS:

Inglesby, Thomas V. "Bioterrorist Threats: What the Infectious Disease Community Should Know about Anthrax and Plague." *Emerging Infections* 5. Washington, DC: American Society for Microbiology Press, 2001.

##### ELECTRONIC:

Central Intelligence Agency. "The Global Infectious Disease Threat and Its Implications for the United States." January 2000. <<http://www.cia.gov/cia/publications/nie/report/nie99-17d.html>> (22 November 2002).

World Health Organization. "Strengthening Global Preparedness for Defense against Infectious Disease Threats." Statement to the United States Senate Committee on Foreign Relations Hearing on The Threat of Bioterrorism and the Spread of Infectious Diseases. 5 September 2001. <[http://www.who.int/emc/pdfs/Senate\\_hearing.pdf](http://www.who.int/emc/pdfs/Senate_hearing.pdf)>(24 November 2002).

##### SEE ALSO

*Biocontainment Laboratories*  
*Biological Warfare*  
 CDC (*United States Centers for Disease Control and Prevention*)  
*L-Gel Decontamination Reagent Pathogens*  
*Public Health Service (PHS), United States*

---

## Anti-Imperialist Territorial Nuclei (NTA)

---

The Anti-Imperialist Territorial Nuclei (NTA) is a small (approximately 20 members) clandestine leftist extremist group that appeared in the Friuli region in Italy in 1995. NTA adopted the class struggle ideology of the Red Brigade of the 1970s-80s and a similar logo—an encircled five-point star—for their declarations. The group opposes what it perceives as U.S. and NATO imperialism and condemns Italy's foreign and labor policies. NTA opposes both the U.S. and the NATO presence in Italy. NTA attacked property owned by U.S. Air Forces personnel at Aviano Air Base. The NTA also claimed responsibility for a bomb attack in September, 2000, against the Central European Initiative office in Trieste and a bomb attack in August, 2001, against the Venice Tribunal building. NTA members threw gasoline bombs at the Venice and Rome headquarters of the then-ruling party, Democrats of the Left, during the NATO intervention in Kosovo.

The NTA operates in northeastern Italy, including the Friuli, Veneto, and Emilia regions.

#### ■ FURTHER READING:

##### ELECTRONIC:

CDI (Center for Defense Information), Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <<http://www.cdi.org/terrorism/terrorist.cfm>> (April 17, 2003).

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001," Annual Report: On the record briefing. May 21, 2002 <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

##### SEE ALSO

*Terrorism, Philosophical and Ideological Origins*  
*Terrorist and Para-State Organizations*  
*Terrorist Organization List, United States*  
*Terrorist Organizations, Freezing of Assets*

---

## APIS (Advance Passenger Information System)

---

The Advance Passenger Information System (APIS) is an electronic database system that stores information about airline travelers. The system, operated by the United States Customs Service, the Immigration and Naturalization Service (INS), and the Federal Aviation Administration (FAA), provides searchable biographical and security information on air travelers entering the United States from a foreign location.

As of March 1, 2003, the newly created United States Department of Homeland Security (DHS) absorbed the former Immigration and Naturalization Service (INS). All INS border patrol agents and investigators—along with agents from the U.S. Customs Service and Transportation Security Administration—were placed under the direction of the DHS Directorate of Border and Transportation Security (BTS). Responsibility for U.S. border security and the enforcement of immigration laws was transferred to BTS.

BTS is scheduled to incorporate the United States Customs Service (previously part of the Department of Treasury), the enforcement division of the Immigration and Naturalization Service (previously part of the Department of Justice), the Animal and Plant Health Inspection Service (previously part of the Department of Agriculture), the Federal Law Enforcement Training Center (previously part of the Department of Treasury), Transportation Security Administration (previously part of the Department of Transportation) and the Federal Protective Service (previously part of the General Services Administration).

Former INS immigration service functions are scheduled to be placed under the direction of the DHS Bureau of Citizenship and Immigration Services. Under the reorganization the INS formally ceases to exist on the date the last of its functions are transferred.

Although the description of the technologies involved in the APIS entry security program remained stable, in an effort to facilitate border security BTS plans envision higher levels of coordination between formerly separate agencies and databases. As of April 2003, the specific coordination and future of the APIS database was uncertain with regard to name changes, database administration, and user policy changes.

Common APIS data includes information that is routinely found on a passport or visa and airline boarding card, such as an individual's name, birth date, country of residence, country of origin and final destination. Records also note if the passenger has been issued a United States visa. In some locations, optical scanners are used to obtain digital records of passports, visas, and other documents.

Although initiated as a voluntary program for air carriers in 1988, anti-terrorism and security legislation passed in the wake of the September 11, 2001 terrorist attacks mandated participation in the APIS. Prior to departure of every international flight bound for the United States, APIS information is checked against the Interagency Border Inspection System (IBIS) database. IBIS is a combined Federal law enforcement database consisting of records from the Department of State, INS, Customs Service, and other agencies. IBIS, when used in conjunction with APIS, prevents entry into the United States by illegal aliens, and persons wanted on visa or customs violations. APIS information is also cross-checked with Federal Bureau of Investigation (FBI) and State Department wanted persons files.

A new voluntary program encourages air carriers to submit APIS manifests for flights departing from the United States for international destinations. The INS is developing and testing various database systems to monitor more closely foreign nationals with U.S. visas. The outbound APIS program allows authorities to confirm when foreign nationals with visas leave the United States when their documents expire. Voluntary APIS is also being used on limited domestic flights.

Since its inception, over 200 million passengers have been processed through the APIS system.

#### ■ FURTHER READING:

##### ELECTRONIC:

Bureau of Citizenship and Immigration Services. INSPASS. March 1, 2003. <<http://www.immigration.gov/graphics/howdoi/inspassloc.htm>> (April 14, 2003).

Department of Homeland Security. April 2, 2003. <<http://www.dhs.gov/dhspublic/index.jsp>> (April 11, 2003).

United States Department of Homeland Security. Immigration Information, INSPASS. March 4, 2003. <<http://www.immigration.gov/graphics/shared/howdoi/inspass.htm>> (April 9, 2003).

United States Department of Homeland Security. Bureau of Citizenship and Immigration Services, PORTPASS. March 11, 2003. <<http://www.immigration.gov/graphics/howdoi/portpass.htm>> (April 9, 2003).

#### SEE ALSO

*IBIS (Interagency Border Inspection System)*

*IDENT (Automated Biometric Identification System)*

*INSPASS (Immigration and Naturalization Service Passenger Accelerated Service System)*

*NAILS (National Automated Immigration Lookout System)*

*PORTPASS (Port Passenger Accelerated Service System)*

*SENTRI (Secure Electronic Network for Travelers' Rapid Inspection)*

## Archeology and Artifacts, Protection of during War

■ ADRIENNE WILMOTH LERNER

Plundering is a practice as ancient as warfare itself. With the development of the world's great civilizations, the proverbial "spoils of war" often included national and cultural treasures, including priceless art and antiquities. The looting of exotic, foreign treasure filled the national coffers and museums of the victorious, while depleting the vanquished of tangible remnants of their history. The evolution of warfare, both technical and philosophical, altered international perceptions on the seizure of cultural goods. However, today's international bans on the looting and trafficking of antiquities, as well as the expectation that cultural sites remain protected during wartime, took three centuries to come to fruition.

### The Colonial Era: The Beginning of Modern Conflicts over Wartime Plunder

The discovery of the New World by European explorers sparked a fierce competition among European nations to obtain territories abroad. Colonialism was fueled by the desire to fill national coffers, through trade, agriculture, or plunder. In the sixteenth and seventeenth centuries, exaggerated rumors of indigenous wealth and stores of gold encouraged plunder of Indian villages. Almost immediately, the demand for exotic objects d'art from the Americas swelled, as wealthy aristocrats clamored for Incan jewelry and Mayan antiquities.



In the 1790s, the birth of the academic discipline of archaeology spurred further interest in antiquities. Archaeologists conducted expeditions, excavating sites and capturing the popular imagination with the artifacts they found. The development of archaeology occurred with a contemporary revival in colonialism. In the early 1800s, independence movements drove European colonial powers from much of the Americas. Seeking other venues for expanding colonial markets, obtaining natural resources, and extending political influence, several European nations, including Britain, France, and the Netherlands, turned to colonial endeavors in Africa and Asia. As imperial powers expanded, so too did public interest in exotic artifacts. During the mid-nineteenth century, Chinese porcelains, costumes, and figurines were popular goods in Holland, Britain, and France. At the turn of the twentieth century, British collectors favored artifacts and antique jewels from Egypt and India. Colonialism provided a means for such cultural resources to be trafficked to Europe for sale or display in museums.

Even in times of warfare, such as the Napoleonic Wars and wars of colonial expansion, cultural resources were a prime consideration. Many western armies freely destroyed indigenous or ancient sites of cultural significance in the heat of battle—a practice that later devastated the many Medieval and Renaissance treasures in Europe itself during World War I. Western archaeologists and antiquities collectors, in an era before the discipline became highly scientific, looted sites to locate artifacts. Antiquities of value were removed from their national contexts, and sent back to museums in Europe. Napoleon employed special spies to locate and gather the best art and antiquities in conquered nations to send back to Paris. In Britain, ancient Egyptian goods and mummies proved immensely popular with collectors and museum audiences. Later, French wars in Indochina created a popular vogue of Buddhist relics and ancient Chinese artifacts.

Even though many of the great finds of the last three hundred years were considered spoils of war or colonialism, the removal of artifacts from their national contexts in the eighteenth and nineteenth centuries was illustrative of the colonial worldview. Many archeologists, antiquities collectors, and museum collectors considered the removal of foreign treasures to European museums a chief means of preservation. They considered themselves better stewards of the world cultural resources, believing that European collections offered better access for scholars, and a safer environment for the storage of the artifacts themselves.

Changing practices in the discipline of archaeology, which is now highly specialized, scientific, and wholly dependent on the provenience (location and context) of cultural goods, and the fall of colonialism, facilitated the end of widespread plundering of African and Far Eastern antiquities to Western museums. The demise of nineteenth century values regarding antiquities, however, raised new questions about the ownership of goods plundered during past conflicts.

One of the most complicated cases in the international dispute over antiquities repatriation, the giving back of antiquities or works of art to their original owner, is that of the British-owned Elgin Marbles. The stone sculptures hail from the Greek Parthenon, but were purchased by Lord Elgin, a British collector, from Greek authorities, shortly before Greece erupted in a decades-long series of wars. The Parthenon was in dubious condition, and Elgin took the statues in an allegedly legal transaction. After the establishment of international laws governing the repatriation of both wartime and peacetime plundered goods, the Greek government appealed to the British History Museum for the return of the Elgin Marbles. The legal battle remains ongoing, intensified by Greece's desire to repossess the statues before the 2004 Olympics in Athens, but Britain has retained ownership of the prized antiquities.

## Plunder and Warfare in the Twentieth Century

In the early twentieth century, the question of wartime plunder of cultural resources came to the fore in Europe. The outbreak of World War I challenged national art and antiquities holdings in a new manner. The advent of total war threatened archaeological sites, buildings, museums, and other national treasures. More intense and powerful weaponry leveled entire cities. Improvements in transportation permitted a more swift, and expansive, invasion force. Long before the fighting of World War I bogged down in the stalemate of the trenches, museum curators in France, Belgium, and Germany endeavored to protect national art and antiquities treasures. At the Louvre, France's premier art and antiquities museum, the staff evacuated the contents of the museum into secret tunnels and antechambers. Some works were sent to various homes throughout France for protection during the war. A special guard force was established to look after the hidden works, and catalog those sent to safe houses. After the Allied victory in 1918, most all of the works were returned to the Louvre, and only a few were captured by German forces or lost.

Plundering of national museums, on both sides of the conflict, was kept to a minimum in Western Europe. However, the fall of the Austro-Hungarian Empire prompted ethnic regional resistance groups to steal some works, many previously plundered from various small nations subsumed into the empire, from Austria. In Russia, the 1917 Revolution prompted wide-scale looting of treasures from deposed aristocrats and the czar's family. Some treasures ended up in Soviet museums, but more were sold to private collectors in the West willing to pay premium prices for the contraband goods. For decades, Soviet intelligence employed special forces to track and locate stolen Russian art treasures, reclaiming many that ended up in private homes and museums in Eastern Europe.

When World War II erupted in Europe in 1939, many governments embarked on well-orchestrated efforts to protect national treasures from wartime plunder. Most nations perceived an acute threat to cultural resources from Nazi Germany. As Nazi Germany grew in power throughout the 1930s, the nation made plunder of the world's antiquities and art treasures a strategic priority. The Nazi government employed archaeologists, art historians, antiquities specialists, and agents of espionage to locate and seize foreign treasures, especially in Egypt and the Middle East. When war broke out in Europe, Nazi invasion plans for neighboring nations included special provisions for the theft of national treasures, and their relocation to Germany. A methodical bureaucratic system was established to facilitate the cataloging of Nazi wartime plunder—ironically, after Germany's defeat, this careful inventory system aided international repatriation and reclamation efforts.

In France, museum staff once again emptied the Louvre in advance of German occupying forces. The most valuable works of the Louvre were sent into hiding in a variety of locations throughout the nation, trafficked by members of the French Resistance. When Nazi agents broke into the museum to plunder their spoils of war, the galleries were largely empty. After the first weeks of the London Blitz, the German bombing campaign against London, British officials moved the international treasures of the nation's famous museums to underground storage and to safe houses in Wales, Northern England, and Scotland. Many European nations sent valuables to the United States, Australia, or neutral Switzerland for protection. Despite the success of Britain and France in protecting national treasures, the Nazi government plundered antiquities throughout Europe, Africa, and the Middle East. Wartime campaigns of total warfare devastated cultural sites in Belgium, France, the Netherlands, Poland, Germany, and Italy.

## The Holocaust: The Great Theft and the Establishment of International Cultural Resource Protections

The Nazis directed their effort to plunder the world's art and antiquities not only against rival nations, but also at Europe's Jews. During the Holocaust, the German government orchestrated not only the systematic execution of Europe's Jewish population, but also the plunder of all of their goods. In Germany, France, and Northern Europe, wealthy Jews possessed extensive collections of art and antiquities. Some were the major benefactors of national museums, and a few were among some of Europe's leading art and antiquities brokers. Holocaust plunder, known as the Great Theft, was less extensively catalogued by German authorities. The plundered goods, formerly

located in private collections, were not catalogued by museums. Thus, the total loss of priceless cultural resources during the Holocaust is immeasurable.

Though the human tragedy of the Holocaust far outweighed devastation to art and antiquities, the Great Theft was addressed in the 1946 Nuremberg Trials of Nazi war criminals. Theft of personal and cultural property was added to the international standards for war crimes in the 1940s. Much of the stolen Holocaust art and antiquities remain in dispute. With few surviving original owners left to claim stolen goods, many items were subsequently repatriated to their nation of origin, returned to the nation of plunder, or were sold in private art markets. However, the theft of cultural resources during the Holocaust prompted the formation of strict international policy regarding the treatment of art and artifacts in times of both war and peace.

**Protecting art, artifacts, and cultural sites today.** A 1970 United Nations Educational, Scientific and Cultural Organization (UNESCO) convention outlined international policy on the protection of artifacts and cultural sites during both war and peacetime. The convention recommended the repatriation of all antiquities, even those acquired from former colonies. In the 1980s, several UN member nations signed a treaty limiting the destruction of cultural sites during military actions. Archaeologists, art scholars, and antiquities specialists successfully lobbied for a ban on the plunder and traffic of illegally obtained artifacts, or removing any antiquities from their context without express permission of national and local governments. INTERPOL now maintains a special force to investigate art and artifact crimes, including those perpetrated during wartime.

A change in war ethos in the West prompted swift reforms of how military campaigns dealt with cultural resources during war. Cultural sites are generally avoided in battle plans, and many governments maintain both civilian and military intelligence forces trained to protect cultural goods. In the recent conflict in Iraq, however, the national museum, containing a vast wealth of antiquities from ancient Mesopotamia, was looted before guard forces were established. The rampant looting raised questions about the enforcement of international anti-theft laws, the effectiveness of military protection, and the readiness of international intelligence forces to track down the stolen goods. Subsequently, many of the artifacts feared initially stolen or lost were recovered from hidden vaults.

The incident in Baghdad also brought to the attention of the international media one of the most basic concerns of preservationists. The growth of the modern antiquities market, and the continued international hunger for plundered goods, has elevated the price of antiquities to enticingly high levels. High prices encourage the looting

of cultural sites by local populations desperate for income. Despite international action, looting has become an increasing local phenomenon, but looters are better connected to dealers and antiquities markets. The Internet aided the proliferation of illegally obtained antiquities, but also helps law enforcement monitor the illegal cultural goods trade.

One of the greatest protections to archaeological sites and cultural resources during wartime is the continued development of “smart weapons,” ammunition that is carefully guided to specific strategic targets and detonated to minimally impact surrounding areas. Smart weapons permit militaries to strike targets in close proximity to cultural sites. Use of smart weapons by Britain and the United States in the Iraq War minimized damage to Baghdad’s numerous museums, mosques, and cultural sites. However, these weapons are only developed, possessed, and used by a handful of the most developed nations. Less developed regions, many of which are prone to endemic conflict, rely on more conventional weapons and techniques of total warfare.

Today, the national governments of the United States, Canada, and the European Union maintain the most comprehensive intelligence forces devoted to the protection of the archaeological and art resources. In 1998, several European nations sent a special task force into the Balkans, in conjunction with UN operations in Bosnia, to track the trafficking and theft of cultural resources. Coalition nations from the Iraq War in 2003 have devoted intelligence resources to an international effort to recover goods stolen from the Iraqi museum. Thus far, the international intelligence community and INTERPOL have arrested persons suspected of trafficking Iraqi treasures in Europe, the United States, and Asia.

#### ■ FURTHER READING:

##### BOOKS:

- Brodie, Neil, and Kathryn Walker Tubb. *Illicit Antiquities: The Theft of Culture and the Extinction of Archaeology*. London: Routledge, 2002.
- Feliciano, Hector. *The Lost Museum: The Nazi Conspiracy to Steal the World’s Greatest Works of Art*. New York: Basic Books, 1987.
- Simpson, Elizabeth. *The Spoils of War: World War II and Its Aftermath: The Loss, Reappearance, and Recovery of Cultural Property*. New York: Abrams, 1997.

##### SEE ALSO

*Architecture and Structural Security*  
*Document Forgery*  
*Espionage and Intelligence, Early Historical Foundations*  
*Forensic Geology in Military or Intelligence Operations*  
*Interpol (International Criminal Police Organization)*  
*Libraries and Information Science (NCLIS), United States National Commission*

*World War I*  
*World War II*

## Architecture and Structural Security

■ JUDSON KNIGHT

Buildings have always stood under the threat of physical attack, but until the advent of organized terrorism in the latter twentieth century, most structural dangers were limited to fires, natural disasters, and acts of war. Since the early 1970s, however, it has become increasingly apparent to authorities in the West that their physical structures are potential targets for terrorist actions, especially bombings, even during peacetime. Such concerns have given rise to efforts by architects, engineers, and planners, sometimes working closely with government security experts, to create structures designed to meet two differing, almost contradictory, needs: security on the one hand, usability and aesthetics on the other.

### Bombings of the 1990s

Among the most notable terrorist bombings of buildings prior to 2001 was the assault on the United States Marine barracks in Beirut, Lebanon, in October 1983, followed a decade later by a string of bombings throughout the 1990s: the first attack on the World Trade Center (WTC) in February 1993; the explosion of the Alfred P. Murrah Federal Building in Oklahoma City in April 1995; the bombing of Khobar Towers in Dharran, Saudi Arabia, in June 1996; and the attack on the U.S. embassies in Kenya and Tanzania in August 1998.

Death tolls differed, from fewer than ten in the case of the first WTC incident to several hundred in the Marine barracks bombing 10 years earlier. And although most of these were perpetrated by Middle Eastern terrorists—albeit from differing groups that collectively represented the breadth of the Islamic fringe—Oklahoma City was an exception, the work of American extremists. Yet, each bombing was alike in terms of basic method: the use of a truck, driven alongside the building or beneath it, to deliver explosives.

**The conflict between comfort and safety.** In order to create structures that could withstand such an attack, designers must confront a classic dilemma of architecture and structural security articulated by Cheryl Kent in the *New York*

*Times*. “At heart, the task involves what seems like a contradiction: designing a building that is secure from attack while affording the openness appropriate for a public building.”

Prior to the 1970s, security was not the paramount consideration in architecture and therefore, comfort and the human touch remained preeminent considerations. Planners of the 1972 Olympic Village in Munich, Germany—wanting to avoid the appearance of an armed camp, with its potential evocations of Hitler and the 1936 Berlin Games—had created an open, friendly village that proved vulnerable to Palestinian terrorists. The subsequent assault by Black September left 11 Israeli athletes and one German policeman dead. Olympic officials learned from Munich and, thenceforth, greatly intensified the security measures surrounding the Games; likewise the planners of government buildings eventually learned from the terrorist attacks of the 1990s.

**The Ronald Reagan building.** The learning process was far from instantaneous, as illustrated by a look at the Ronald Reagan Building in Washington, D.C. It was completed in July 1997, a year after the Khobar Towers and a year before the Africa bombings. The first World Trade Center bombing and Oklahoma City were still fresh in memory as evidence that terrorism was no longer a phenomenon from which Americans on U.S. soil were exempt. Yet, a 1999 report by security experts at Sandia National Laboratories found that the building, which had run well over budget to finish at \$818 million, was “highly vulnerable” to terrorist attack.

Several factors made the vulnerability of the Reagan Building particularly dismaying. There was its proximity to the White House and Capitol, combined with the large numbers of employees to be housed there. Additionally, it would serve as the headquarters of sensitive agencies such as the U.S. Customs Service, and the venue of high-security events such as the North Atlantic Treaty Organization 50th anniversary celebrations in April, 1999. Yet, the GSA, hoping to defray some of the costs by leasing space to the private sector for restaurants, shops, and convention facilities, had wanted to avoid creating a building that looked like an armed fortress.

**The Oklahoma City Federal Campus.** By contrast, a Chicago architectural firm managed to create a secure environmental—yet one that did not seem constricting to its inhabitants or visitors—in their design for Oklahoma City’s Federal Campus. The new name was chosen to avoid any reference to “Federal Building,” a term forever associated in local minds with the structure in Oklahoma City that had been destroyed, along with 168 people.

Design architects planned the site in such a way that, rather than lying hidden behind a protective plaza, the building fills the block on which it sits. This has the added

benefit of addressing an aesthetic problem in the Oklahoma City downtown, which, like that of other sunbelt cities such as Atlanta or Houston, is pockmarked with empty lots. By building to the boundaries of the site, the Federal Campus conveys a sense of a populated environment that serves to invite traffic. Welcoming traffic was also apparently in the architects’ considerations when they fought off security planners’ attempts to close off streets around the building, a measure that might have kept away the public.

One of the few obvious signs of protective considerations in the design is the lack of glass in the outer perimeter of the Federal Campus. The building does have extensive glass areas, but these are inside the protected courtyard, and the glass itself is reinforced—rather like that of a car windshield—so that it would shatter rather than break in the face of concussive force. Walls on either side of the lobby are made to create a powerful aesthetic effect, while protecting office workers in the event of an explosion.

## Designing and Protecting the Post-September 11, 2001, World

Ironically, in its September, 2001 issue, which went to press before the bombings, *Signal* reported that GSA was testing a risk assessment and property analysis software product called RAMPART as a means of determining buildings’ vulnerabilities to terrorism. Designed at Sandia, RAMPART made it possible to study a number of threats, both natural and manmade, and allowed users to assess buildings with a point-and-click walk-through assessment tool that took less than two hours.

After the World Trade Center terrorist attack, the idea that such software could get into the wrong hands prompted a joint statement by the American Institute of Architects (AIA) and the GSA to immediately report any suspicious requests to the appropriate local FBI field office. Just as terrorists’ strange requests at flight schools—e.g., their desire to learn how to fly a plane, but not how to land—should have, and in some cases did raise red flags, the AIA and GSA warned architects, engineers, and others concerning requests for intricately detailed plans of major buildings.

Months earlier, an AIA member firm had received several e-mail messages from an alleged student in Egypt who requested plans that would show extremely specific information about conduits, duct work, wiring, risers, and other aspects of a particular building. Acting with prescience (given that this was before September 11), the firm turned the requests over to the FBI. The wisdom of such measures became all the more apparent after the March, 2003, capture of Khalid Sheikh Mohammed, a high-ranking al Qaeda figure who revealed that plans were in the works for attacks on structures ranging from the White

House and Israeli embassy in Washington, D.C. to bridges in Manhattan and the Sears Tower in Chicago.

In December, 2001, the FBI revealed that the World Trade Center terrorists might have actually used commercially available software to plot the destruction of the towers. Several hundred such programs were on the market at that time, although fewer than half a dozen would have been capable of portraying the effects of a plane crash in any detail.

**Studying how the towers fell.** During late 2001 and 2002, government and private investigators undertook studies to understand how a jetliner could have caused the collapse of the towers. Quickly, the investigators, including representatives of the American Society of Civil Engineers and the Federal Emergency Management Agency (FEMA), concluded that it was not the impact, but the heat from the burning jet fuel that weakened the steel. The National Institute of Standards and Technology (NIST), which later did its own study, found that the temperatures were not high enough to actually melt the steel, as had been originally assumed. The temperatures were sufficient however, to weaken the steel beams, which crumbled at the impact levels of the towers and, in turn, resulted in weight loads sufficient to crush the floors remaining below, resulting in the total collapse of the structures.

Those involved in the World Trade Center site investigation also attributed part of the buildings' vulnerability to what had also been their strength, the use of exterior walls as support. In older skyscrapers such as the Empire State Building, support was at the building's core. This thicket of massive steel girders not only took up rentable interior space, but they had their structural shortcomings, including the fact that they did not prevent a building from swaying in the wind. In the WTC, the exterior columns were linked to the core with steel trusses that had been inadequately fireproofed in the building process. Surrounded only by light foam fireproofing and walled off with sheetrock rather than concrete, the trusses at the impact site were easily exposed by the twin plane crashes, leaving them vulnerable to melting or loss of integrity.

**Building for the future.** The GSA approved a wide range of designs in December, 2001, that seemed to have already taken into account the World Trade Center tragedy three months before. In fact, these were the result of the same post-Oklahoma City studies that yielded the Federal Campus earlier.

Among the \$6 billion worth of projects released in a flurry of GSA approvals was a district courthouse for Miami. Unlike the Federal Campus, this building did sit back from the street, with the intervening space hosting an arboretum. Yet, the arboretum served a security purpose, and not only because it separated the building from the street. "Even if a truck got through the trees," architect

Bernardo Fort-Brescia of Arquitectonica, the design firm, told the *Wall Street Journal*, "they would hit this undulating lawn. We've created an invisible barrier in the sense that it doesn't look like a wall."

Another courthouse, in Springfield, Massachusetts, solved the conflict of security versus aesthetics in a different fashion. Planners wanted local citizens to visit the courthouse frequently for community events, and if attendees had to pass through magnetometers and checkpoints upon entering, this would create a decidedly unfriendly environment. Instead, they separated the entry pavilion from the interior portion, with its security checkpoints hidden from view.

At the new headquarters for the Bureau of Alcohol, Tobacco, and Firearms (ATF) in Washington, designers had dealt with the problem of bollards, the stubby concrete posts that prevent vehicles from driving into buildings at street level. Although useful for security, they are typically far from pleasing visually, yet the architects of the ATF building managed to create bollards that were an exception to the rule. "Instead of looking like dragon's teeth," GSA commissioner for public buildings F. Joseph Moravec told the *Journal*, "there will be some really cool metal bollards. They'll have an antique, almost Edwardian look."

In at least one spot in Washington, D.C., the GSA's "post-9/11" design criteria had been implemented before the World Trade Center attacks. This was the Pentagon, where architects of a remodeling project had used new techniques and materials intended to ensure that, in the event of a devastating attack, the building section would collapse progressively, rather than in a heap. Architects had also used shatterproof glass and other materials because, as Moravec noted, "One of the terrible lessons of Oklahoma City was that when a bomb goes off near a building, it's not so much the blast that kills people. It's that the explosion creates flying elements, pieces of walls and glass that kill." In the remodeled portion of the Pentagon, "When the blast hit the wall, the wall itself didn't become a weapon. There's no question that the glass panels there saved a lot of lives."

#### ■ FURTHER READING:

##### PERIODICALS:

- Aveni, Madonna. "Software Analyzes Potential Threats to Buildings." *Civil Engineering* 71, no. 10 (October 2001): 36.
- Brouwer, Greg. "Oklahoma City Complex Will Usher in New Design Criteria." *Civil Engineering* 72, no. 3 (March 2002): 16.
- Dunlap, David W. "Architects Put on the Alert over Requests That Are Rare." *New York Times*. (October 4, 2001): B8.
- Grant, Peter. "Plots and Ploys." *Wall Street Journal*. (December 26, 2001): B4.
- Kent, Cheryl. "A Safer Federal Building for Oklahoma City." *New York Times*. (August 22, 1999): 34.
- Ottaway, David B. "Reagan Building Vulnerable to Attack." *Washington Post*. (March 8, 1999): A1.

"RAMPART Assesses Threats." *Signal* 56, no. 1 (September 2001): 7.

Salamon, Julie. "A Detective-Story Approach to the Twin Towers' Collapse." *New York Times*. (April 30, 2002): E1.

Smith, Ray A. "The Aesthetics of Security—Building Owners, Architects Seek to Make Properties Safer Without Look of a Fortress." *Wall Street Journal*. (February 19, 2003): B1.

Solis, Suzanne Espinosa. "Software May Have Mapped N.Y. Hit." *San Francisco Chronicle*. (December 12, 2001): A11.

Watts, John M., Jr. "Our Changing World." *Fire Technology* 38, no. 2 (April 2002): 99–100.

#### SEE ALSO

*Computer Modeling*

*FEMA (United States Federal Emergency Management Agency)*

*General Services Administration, United States*

*Kenya, Bombing of United States Embassy*

*Khobar Towers Bombing Incident*

*NIST (United States National Institute of Standards and Technology)*

*Sandia National Laboratories*

*September 11 Terrorist Attacks on the United States*

*World Trade Center, 1993 Terrorist Attack*

## Area 51 (Groom Lake, Nevada)

Area 51 is the popular name of a secret military facility at Groom Lake, Nevada, approximately 90 miles north of Las Vegas. The 6-by-10 mile rectangular air base lies within the Switzerland-sized boundaries of Nellis Air Force Base, and has served as a testing ground for "black budget" (top-secret) military prototype aircraft since the mid-1950s. Area 51 is also a well-known folk symbol of an assumed government conspiracy to cover up information on UFOs and extraterrestrial life.

The United States government has never publicly discussed the existence or purpose of the Groom Lake base, but historical accounts chronicle the site's long history as a preliminary testing ground for the U.S. military's most secret aircraft. The U-2 Spy plane, A-12 and SR-71 Blackbird supersonic reconnaissance jets, and F-117A and B-2 Stealth fighters were all tested at the site before production, as was a reverse-engineered version of a Vietnam War-era Russian MIG-21. Development and testing of secret military aircraft and Unmanned Aerial Vehicles (UAVs) likely continues at Area 51 today.

The secrecy surrounding Groom Lake has piqued public interest since 1955, when the Central Intelligence Agency and Lockheed Skunk Works chose the remote desert area as a testing ground for the U-2. President Eisenhower signed Executive Order 10633 to restrict a

rectangle of airspace over the base that year, and the Department of the Interior withdrew a 60-square-mile rectangle of land beneath the airspace from public use in 1958. Today, the so-called "Groom box" includes a 22-by-20 nautical mile rectangle of restricted airspace, the original 60 square mile base, and a large area of surrounding land with enforced public entry and viewing restrictions.

The present popular fascination with Area 51 bloomed in 1989 when KLAS-TV in Las Vegas broadcast a series of interviews with Robert Lazar, a self-proclaimed aerospace engineer who maintained that he had been hired to help reverse-engineer an alien spacecraft at the Papoose Lake facility near Groom Lake. Lazar asserted that the United States government had recovered a downed extraterrestrial spacecraft and stored it in an underground bunker at Area 51. Lazar's bizarre story elicited support from the community of UFO and alien conspiracy theorists based in Roswell, New Mexico, and ignited public curiosity. The April 1994 issue of *Popular Science* magazine carried a satellite image of Groom Lake on its cover and featured an in-depth article on the military history of the facility. Since then, Area 51 has become a science-fiction staple. The site played a role in several episodes of the FOX television's popular series "The X-Files" and was featured in the 1996 movie "Independence Day." Though the United States military often collaborates with the entertainment industry, it has never sanctioned a project involving Area 51.

#### ■ FURTHER READING:

##### BOOKS:

Rich, Ben and Leo Janos. *Skunk Works*. New York: Bantam, 1994.

##### ELECTRONIC:

Area 51 Research Center. "Area 51: Military Facility, Social Phenomenon and State of Mind." Glenn Campbell. January, 2000. <<http://www.ufomind.com/area51/>> (December 5, 2002).

*Airmen, Magazine of the United States Air Force*. "Flights, Camera, Action!" June, 1997. <<http://www.af.mil/news/airman/0697/index.html>> (December 5, 2002).

#### SEE ALSO

*Aviation Intelligence, History*

*Stealth Technology*

*Unmanned Aerial Vehicles (UAVs)*

## Argentina, Intelligence and Security

Since gaining its independence from Spain in 1816, Argentina has struggled to maintain stable, democratic rule.

Conflict between the military and government factions is endemic. In 1946, the election of President Juan Domingo Peron began a period of authoritarian rule and heightened tensions between military and civilian forces. A military junta overthrew the government again in 1976. Both regimes employed civilian and military intelligence agencies in domestic espionage against Argentinean citizens and persecuted political dissidents. Democratic rule was restored in 1983. The new government overhauled government structure, separating civilian and military agencies into specialized, relatively autonomous units. In 1992, the government modernized and redesigned the nation's intelligence system.

Argentina's intelligence community is divided into civilian and military branches. The civilian intelligence system operates under the direction of the executive branch of the government. The keystone of this network is the National Intelligence Center (CNI). The CNI is responsible for gathering information from various intelligence agencies and coordinating daily operations. In recent years, however, the power of the CNI has greatly diminished. The Office of the State Intelligence Secretary (SIDE) assumed many CNI duties.

SIDE is the oldest Argentinean intelligence agency. Reporting directly to the President, SIDE is charged with culling domestic and foreign intelligence information with which to brief members of the executive branch. The agency also directs the nation's counterintelligence program.

Domestic security was the primary concern of Argentinean legislators who pushed for intelligence reform in the early 1990s. To this end, passage of the Internal Security Law of 1992 created the domestic security service, the National Direction of Internal Intelligence. The agency, a subsidiary of the Ministry of the Interior, created national security policy and coordinates the protection of national interests with the aid of intelligence services and law enforcement agencies, such as the National Gendarmerie and Federal Police.

Military intelligence is coordinated by the Joint Staff of the Armed Forces, and a subcommittee known as J-2 Intelligence. The committee reports to the executive, and like all military intelligence organizations is subject to congressional oversight review, but remains largely autonomous. Each branch of the Argentinean military, the Air Force, Army, and Navy, maintains its own intelligence services.



A car moves along the Extraterrestrial Highway, a roadway that runs along the eastern border of Area 51, a military base on the Nevada test site that the U.S. government has only recently admitted "officially" exists. AP/WIDE WORLD PHOTOS.

In 2002, Argentina again began a period of political instability, in large part due to an economic crisis gripping the country. Until government stability is restored, the future of Argentina's intelligence agencies is uncertain. As in past periods of unrest, military intelligence and security agencies have gained power and influence, eliciting the concern of Argentinean civilians and members of the international community.

## Argonne National Laboratory

■ K. LEE LERNER

Argonne National Laboratory is operated by the University of Chicago for the U.S. Department of Energy (DOE). Located in Argonne, Illinois, the lab is divided operationally into five principle divisions: Physical, Biological & Computing Sciences; Advanced Photon Source; Energy & Environmental Science & Technology; Engineering Research; and Operations.

Argonne scientists collaborate on several projects related to nuclear safety. Argonne's International Nuclear Safety Center (INSC) is dedicated to improving safety related technology and safety protocols for nuclear reactors—including reactors in the former Soviet Union. Funded by DOE's Office of Nonproliferation and National Security, INSC scientists maintain an extensive database related to a variety of nuclear facilities. The INSC database is organized so that researchers can quickly access site-specific information on reactors around the world.

Argonne scientists provide technical support to several agencies involved in stemming proliferation or use of weapons of mass destruction. As of 2003, Argonne's national security related programs supported research dedicated to developing technology—and providing expert guidance—related to arms control and nuclear, chemical, and biological counter-terrorism.

Argonne developed technologies include methods to track nuclear fuels and to support nuclear waste cleanup of spent fuels.

Argonne scientists have developed an electrometallurgical treatment process to handle spent nuclear fuels. The treatment process uses electrorefining techniques that separate uranium, radioactive wastes, and inert materials in sodium bonded metallic fuels. In preparing nuclear waste for disposal, the electrometallurgical treatment process allows the isolation and removal of uranium and also allows the remaining waste into a ceramic or a metal alloy by heating and compressing a composite of borosilicate glass and zeolite (a mineral that incorporates fission waste products). Components of the metal alloy are derived from the steel cladding used to encase the fuel in the reactor. By restricting plutonium access—binding it with

waste products—the plutonium is placed in a form that reduces or eliminates its potential use in a nuclear weapon.

In support of several agencies, Argonne scientists are capable of providing field measurements of radiation exposure dangers and of guiding decontamination efforts associated with reactor decontamination and decommissioning. Part of the decommissioning effort is dedicated to ensuring safe disposal of nuclear fuels so that the fuels can not be used to manufacture nuclear weapons.

Argonne engineers collaborate on efforts to develop sensitive detectors capable of identifying concealed nuclear materials.

Argonne personnel provide technical expertise to Federal Bureau of Investigation counterterrorism operations and aid in domestic infrastructure assurance programs designed to improve security at critical U.S. infrastructure sites. For example, Argonne's PROTECT system, developed by the Decision and Information Sciences Division, features an integrated detection, communication and response program to secure subways against chemical attacks.

Argonne research also includes efforts to improve instruments and sensors capable of detecting chemical and biological agents. As a part of the Joint Chemical Aid Detector Program, Argonne researchers developed portable cyanide-gas microsensors. Engineers are especially interested in developing hypersensitive detectors capable of identifying trace evidence of dangerous chemical or biological agents and developed a series of portable biochip microarrays that are capable of detecting bioagents, including anthrax bacterium.

Argonne's Advanced Photon Source (APS) allows study of the 3-D structure of toxins—including Anthrax toxins. Micro Array of Gel-Immobilized Compounds or MAGIC chips were developed by Argonne researchers to identify biological pathogens and disease related genetic mutations.

### ■ FURTHER READING:

#### ELECTRONIC:

Environmental Measurements Laboratory. National Security. <<http://www.eml.doe.gov/>> (March 16, 2003).

United States Department of Energy, Office of Science. National Laboratories and User Facilities. <[http://www.sc.doe.gov/Sub/Organization/Map/national\\_labs\\_and\\_userfacilities.htm](http://www.sc.doe.gov/Sub/Organization/Map/national_labs_and_userfacilities.htm)> (March 23, 2003).

United States Department of Homeland Security. Research & Technology. <<http://www.dhs.gov/dhspublic/display?theme=27&content=374>> (March 23, 2003).

#### SEE ALSO

*Brookhaven National Laboratory*  
*DOE (United States Department of Energy)*  
*Environmental Measurements Laboratory*  
*Lawrence Berkeley National Laboratory*  
*Lawrence Livermore National Laboratory (LLNL)*  
*Los Alamos National Laboratory*





President Bush, center, gets a look at new weapons in the war on terror during a visit to the Argonne National Laboratory in Argonne, Illinois. AP/WIDE WORLD PHOTOS.

*NNSA (United States National Nuclear Security Administration)  
Oak Ridge National Laboratory (ORNL)  
Pacific Northwest National Laboratory  
Plum Island Animal Disease Center  
Sandia National Laboratories*

## Armed Islamic Group (GIA)

An Islamic extremist group, the Armed Islamic Group (GIA) aims to overthrow the secular Algerian regime and replace it with a fundamentalist Islamic state. The GIA began its violent activity in 1992 after Algiers voided the victory of the Islamic Salvation Front (FIS)—the largest Islamic opposition party—in the first round of legislative elections in December 1991.

**Organization activities.** GIA frequently attacks civilians and government workers in Algeria. Between 1992 and 1998,

the GIA conducted a terrorist campaign of civilian massacres, sometimes wiping out entire villages in its area of operation. Since announcing its campaign against foreigners living in Algeria in 1993, the GIA has killed more than 100 expatriate men and women—mostly Europeans—in the country. The group uses assassinations and bombings, including car bombs, and it is known to favor kidnapping victims and slitting their throats. The GIA hijacked an Air France flight to Algiers in December 1994. In late 1999, a French court convicted several GIA members for conducting a series of bombings in France in 1995.

Precise numbers of the GIA members are unknown, but are estimated at about 200 members. Algerian expatriates, some of whom reside in Western Europe, provide some financial and logistic support to GIA. In addition, the Algerian government has accused Iran and Sudan of supporting Algerian extremists.

### ■ FURTHER READING:

#### ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001, Annual Report: On the record briefing. May 21, 2002 <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17,2003).

U.S. Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

#### SEE ALSO

*Terrorism, Philosophical and Ideological Origins  
Terrorist and Para-State Organizations  
Terrorist Organization List, United States  
Terrorist Organizations, Freezing of Assets*

---

## Arms Control, United States Bureau

---

The Bureau of Arms Control is an office of the United States Department of State devoted to policy on military arms of all types, from conventional to nuclear. It falls under the U.S. Arms Control and Disarmament Agency, which Congress placed under State Department control in 1999. Among its functions is the implementation of existing arms agreements. The bureau also serves the secretary of state in an advisory capacity, providing the secretary with information on a variety of national security issues related to arms control.

The Bureau of Arms Control was a product of the merger between the United States Arms Control and Disarmament Agency (created by Congress in 1961) and the State Department on April 1, 1999. Thenceforth, the newly created bureau, along with the bureaus of Nonproliferation, Verification and Compliance, and Political-Military Affairs, would be subordinate to the undersecretary of state for Arms Control and International Security. Answering to the undersecretary on behalf of the Bureau of Arms Control is an assistant secretary.

Areas of responsibility for the Bureau of Arms Control include developing policy with regard to use of conventional, chemical/biological, and nuclear forces and arms. The bureau is also charged with supporting negotiations for arms control agreements, and for implementing existing agreements. It further supports the secretary of state on relevant national security issues, such as those involving testing of nuclear weapons or the development of missile-defense systems.

The bureau's mission extends beyond these responsibilities, however, to the most creative area in the field of arms control: the negotiation of new agreements. For example, the bureau helped lead efforts toward the creation of the Moscow Treaty on strategic offensive reductions in May 2002.

#### ■ FURTHER READING:

##### BOOKS:

Butler, Richard. *The Greatest Threat: Iraq, Weapons of Mass Destruction, and the Crisis of Global Security*. New York: Public Affairs, 2000.

Forsberg, Randall. *Nonproliferation Primer: Preventing the Spread of Nuclear, Chemical, and Biological Weapons*. Cambridge, MA: MIT Press, 1995.

##### ELECTRONIC:

U.S. Department of State Bureau of Arms Control <<http://www.state.gov/t/ac/>> (December 30, 2002).

#### SEE ALSO

*NNSA (United States National Nuclear Security Administration)*

---

## Army for the Liberation of Rwanda (ALIR)

---

The Army for the Liberation of Rwanda (ALIR) also operates as, or is known as, Interahamwe, Former Armed Forces (ex-FAR).

The FAR was the army of the Rwandan Hutu regime that carried out the genocide of 500,000 or more Tutsi and regime opponents in 1994. The Interahamwe was the civilian militia force that carried out much of the killing. The groups merged and recruited additional fighters after they were forced from Rwanda into the Democratic Republic of Congo (then Zaire) in 1994. They are now often known as the Army for the Liberation of Rwanda (ALIR), which is the armed branch of the PALIR or Party for the Liberation of Rwanda. The group seeks to topple Rwanda's Tutsi-dominated government, reinstitute Hutu-control, and, possibly, complete the genocide. In 1996, a message allegedly from the ALIR threatened to kill the United States ambassador to Rwanda and other U.S. citizens. In 1999, ALIR guerrillas, critical of alleged U.S.-U.K. support for the Rwandan regime, kidnapped and killed eight foreign tourists including two U.S. citizens in a game park on the Congo-Uganda border. In the current Congolese war, the ALIR is allied with Kinshasa against the Rwandan invaders. Several thousand ALIR regular forces operate alongside the Congolese army on the front lines of the Congo civil war, while a like number of ALIR guerrillas operates behind Rwandan lines in eastern Congo closer to the Rwandan border and sometimes within Rwanda.

FAR generally operates in the Democratic Republic of the Congo and Rwanda, but has operated in Burundi. The Democratic Republic of the Congo provides ALIR forces in Congo with training, arms, and supplies.

■ FURTHER READING :

ELECTRONIC:

CDI (Center for Defense Information), Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <<http://www.cdi.org/terrorism/terrorist.cfm>> (April 17, 2003).

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001," Annual Report: On the record briefing. May 21, 2002 <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

SEE ALSO

*Terrorism, Philosophical and Ideological Origins*  
*Terrorist and Para-State Organizations*  
*Terrorist Organization List, United States*  
*Terrorist Organizations, Freezing of Assets*

## Army Medical Research Institute of Chemical Defense (USAMRICD).

SEE *USAMRICD (United States Army Medical Research Institute of Chemical Defense)*.

## Army Medical Research Institute of Infectious Diseases (USAMRIID).

SEE *USAMRIID (United States Army Medical Research Institute of Infectious Diseases)*.

---

## Army Security Agency

---

■ JUDSON KNIGHT

The Army Security Agency (ASA) provided the United States Army with signal intelligence and security information from 1945 to 1976. During the 1960s, ASA played a key role in the Vietnam conflict, a role symbolized by the fact that an ASA operative was the first soldier killed in the war.

For almost as long as there has been viable electronic communication, the U.S. military has been concerned with the field of signals intelligence (SIGINT): information gathered from the interception, processing, and analysis of electronic communications. The first SIGINT efforts in World War I were informal, and only in 1930 did the army organize the first permanent SIGINT organization, the Signal Intelligence Service (SIS).

In 1943, the army renamed SIS as the Signal Security Agency, or SSA. On September 15, 1945, less than two weeks after the end of World War II, SSA became the Army Security Agency. Commanded by the director of military intelligence for the army, the newly formed office possessed broad powers, a fact made evident by its wide geographic presence: in addition to untold fixed sites, or field stations, across the globe, it also maintained significant theatre headquarters in both Europe and east Asia.

Four years after its formation, in 1949, the ASA was placed—along with its navy and air force counterparts—under the new Armed Forces Security Agency (AFSA). Though AFSA was a forerunner of the National Security Agency (NSA; formed in 1951), unlike NSA, AFSA had little actual power. Therefore, the reorganization had little effect on ASA operations other than the reassignment of most ASA civilian personnel to AFSA. ASA, meanwhile, continued its duties in the field, and would play a key intelligence role in the conflicts of the 1950s and 1960s.

### ASA in Korea and Vietnam

As a result of needs created by the Korean War, ASA expanded its operations, and deployed numerous tactical units to support the army on the ground. The Korean conflict saw the first use of groups and battalions in the ASA structure, a symbol of its growth during wartime. In 1955, ASA expanded its mission to include electronic intelligence and electronic warfare functions that had formerly been the responsibility of the signal corps. Because its role now encompassed more than intelligence and security, it was reassigned from G-2 (military intelligence) to the U.S. Army chief of staff.

The first ASA personnel arrived in Vietnam on May 13, 1961, to set up a post at Tan Son Nhut Air Base in South Vietnam. Assigned to the 3rd Radio Research Unit (RRU), ASA personnel were chiefly concerned with direction-finding (DF) operations to locate Viet Cong transmitters operating in South Vietnamese territory. On December 22, 1961, a Viet Cong ambush outside the capital city of Saigon claimed the life of Specialist Fourth Class James T. Davis, a DF operator who became the first of more than 50,000 American soldiers killed in Vietnam during the next 11 years.

Davis's death pointed up the dangers for the DF operator in Vietnam: because of the difficulties of wave propagation in the thick southeast Asian jungles, the DF operator had to be close to the transmitter to detect it. The solution was an airborne DF platform, the first of which ASA deployed in March 1962. In 1965, as the U.S. presence in Vietnam reached its height, the 509th Radio Research Group replaced the 3rd RRU, and ASA personnel in country numbered as many as 6,000. The agency itself had grown to include some 30,000 personnel, and in 1964 had become a major army field command.

As the Vietnam conflict drew to a close, however, ASA began to contract rapidly. By 1975, reorganization

had effectively ended its existence, and it was formally disbanded on the last day of 1976. On January 1, 1977, a new security and intelligence command known as Headquarters, U.S. Army Intelligence and Security Command, replaced ASA.

#### ■ FURTHER READING:

##### BOOKS:

Bamford, James. *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency: From the Cold War through the Dawn of a New Century*. New York: Doubleday, 2001.

##### ELECTRONIC:

Army Security Agency Online. <<http://www.asa.npoint.net>> (December 30, 2002).

Origins of the Army Security Agency and INSCOM. <[http://www.nsa.gov/display/c130/ru8\\_asa.html](http://www.nsa.gov/display/c130/ru8_asa.html)> (December 30, 2002).

##### SEE ALSO

*Codes and Ciphers*  
*Cryptology, History*  
*SIGINT (Signals Intelligence)*

---

## 'Asbat al-Ansar

---

'Asbat al-Ansar—the Partisans' League—is a Lebanon-based, Sunni extremist group, composed primarily of Palestinians, which is associated with Osama Bin Ladin. The group follows an extremist interpretation of Islam that justifies violence against civilian targets to achieve political ends. Some of those goals include overthrowing the Lebanese government and thwarting perceived anti-Islamic influences in the country.

**Organization activities.** 'Asbat al-Ansar has carried out several terrorist attacks in Lebanon since it first emerged in the early 1990s. The group carried out assassinations of Lebanese religious leaders and bombed several nightclubs, theaters, and liquor stores in the mid-1990s. The group raised its operational profile in 2000 with two dramatic attacks against Lebanese and international targets. The group was involved in clashes in northern Lebanon in late December, 1999, and carried out a rocket-propelled grenade attack on the Russian embassy in Beirut in January 2000.

'Asbat al-Ansar commands about 300 hundred fighters in Lebanon. The group's primary base of operations is the 'Ayn al-Hilwah Palestinian refugee camp near Sidon in southern Lebanon, and it is thought that they receive money through international Sunni extremist networks and Osama Bin Ladin's al-Qaida network.

#### ■ FURTHER READING:

##### ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001, Annual Report: On the record briefing. May 21, 2002 <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

##### SEE ALSO

*Terrorism, Philosophical and Ideological Origins*  
*Terrorist and Para-State Organizations*  
*Terrorist Organization List, United States*  
*Terrorist Organizations, Freezing of Assets*

---

## Asilomar Conference

---

Soon after the discovery in 1970 of the first restriction enzyme by American microbiologist Hamilton Smith, it became possible to combine DNA from different sources into one molecule, producing recombinant DNA. Concern by scientists and lay people that some of this recombinant technology DNA might be harmful to humans—either by unintentional or deliberate release or recombinant DNA into the environment—prompted the research to stop until scientists could evaluate its risks.

In February 1975, over 100 internationally respected molecular biologists met at the Asilomar conference center in California. There, they decided upon a set of guidelines to be followed by all scientists doing recombinant DNA research. They considered each class of experiments, and assigned it a level of risk: minimal, low, moderate, or high. Each level of risk required a corresponding set of containment procedures designed to minimize the chance of vectors (carriers) containing recombinant DNA molecules from escaping into the environment where they could potentially harm humans or other parts of the ecosystem. Because these projected experiments had never been done, assignment to a risk category was, of course, somewhat speculative and subjective. Accordingly, the potential risks were arrived at by estimate.

At all risk levels, the guidelines called for the use of biological barriers. Bacterial host cells should be from strains unable to survive in natural environments (outside the test tube). Vectors carrying recombinant DNA, including plasmids, bacteriophages, and other viruses, were to be nontransmissible and also unable to survive in natural environments.

For experiments having minimal risk, the guidelines recommended that scientists follow general microbiology

safety procedures. These included not eating, drinking, or smoking in the lab; wearing laboratory coats in the work area; and promptly disinfecting contaminated materials.

Low risk procedures required a bit more caution. For example, procedures producing aerosols, such as using a blender, were to be performed under an enclosed ventilation hood to eliminate the risk of the recombinant DNA being liberated into the air.

Moderate risk experiments required the use of a laminar flow hood, the wearing of gloves, and the maintenance of negative air pressure in the laboratory. This would ensure that air currents did not carry recombinant DNA out of the laboratory.

Finally, in high risk experiments, maximum precautions were specified. These included isolation of the laboratory from other areas by air locks, having researchers shower and change their clothing upon leaving the work area, and the incineration of exhaust air from the hoods.

Certain types of experiments were not to be done at all. These most potentially dangerous experiments included the cloning of recombinant DNA from highly pathogenic organisms or DNA containing toxin genes. Also forbidden were experiments involved the production of more than 10 liters of culture using recombinant DNA molecules that might render the products potentially harmful to humans, animals, or plants.

The scientists at the Asilomar conference also resolved to meet annually to re-evaluate the guidelines. As new procedures were developed and safer vectors and bacterial cells became available, it became possible to re-evaluate and relax some of the initially stringent and restrictive safety standards.

#### ■ FURTHER READING:

##### PERIODICALS:

Barinaga, Marcia, "Asilomar Revisted: Lessons for Today?" *Science* 287 (2000).

##### SEE ALSO

*Biocontainment Laboratories*  
*Biodetectors*  
*Biological Weapons, Genetic Identification*  
*DNA Fingerprinting*  
*DNA Recognition Instruments*  
*DNA Sequences, Unique*

## Assassination

#### ■ JUDSON KNIGHT

Assassination is a sudden, usually unexpected act of murder committed for impersonal reasons, typically with a

political or military leader as its target. Although assassination gained its name from that of a fanatical Near Eastern sect in the Middle Ages, the practice of assassination goes back to ancient times, and extends to the present day. At one time, the most widely used tool for assassination was a knife or dagger, whereas modern assassinations more often use guns or bombs, while poisons have long been a means of political killing.

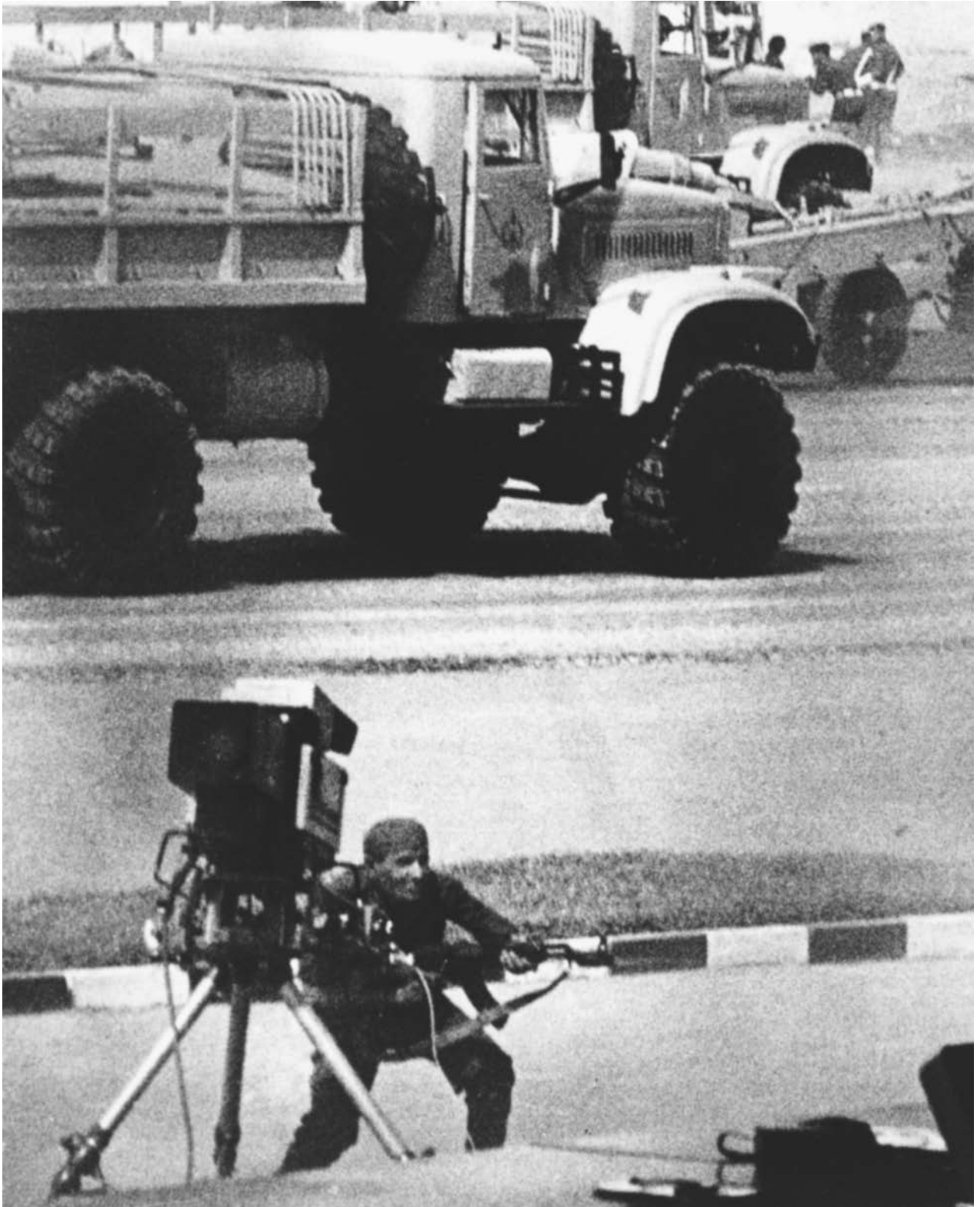
### Assassination in History

The first significant assassination victim was probably the Egyptian pharaoh Amenemhet I, who established the Twelfth Egyptian Dynasty in 1986 B.C. Amenemhet gained his power by an act of usurpation, thus perhaps setting an example for a group of courtiers who conspired in his killing. Six centuries later, Horemhab, a general who competed with the grand vizier Aya for the hand of Tutankhamen's widow (and hence for the political legitimacy to be gained by marrying a queen), was likewise a victim of assassination—in this case, by his rival.

The list of assassination victims in ancient times is far too long to recount in detail. Roman history alone is studded with acts of murder. Long before and after the most famous assassination in Rome's history—that of Julius Caesar in 44 B.C.—the dagger proved a far more common instrument of political change than the ballot. The assassination of Domitian in A.D. 96, and that of Commodus in 192, serve as virtual bookends to the golden age of the empire, after which the western portion fell into a slow, but steady decline. During the half-century that began in 235, no fewer than 20 men held and lost the seat of Roman power, more often than not at the hands of assassins.

Assassination plots, or rumors of them, have sometimes had the effect of neutralizing a ruler indirectly. Some of the greatest and most despicable men of ancient times—Hannibal on the one hand, and Nero on the other—killed themselves rather than let assassins do the job. And Chandragupta, founder of the Mauryan empire of India in the third century, feared assassination so much that in 301 he left his throne, joined the Jain sect, and later died of starvation.

On the other hand, rulers secure in their power usually dealt severely with would-be assassins. Such is the case with the ruthless Prince Cheng of China's Ch'in state during the third century B.C. Many people wanted the tyrant Cheng dead, and the crown prince of the rival Yan kingdom set in motion assassination plans. It was a mark of the terror Cheng commanded that the king of Yan killed his own crown prince in the hope that it would please the Ch'in ruler. Although history does not record Cheng's response to this favor, the event marks one of those junctures in which assassination could or would have altered history: Cheng went on to unite China, which today



A gunman wearing an Egyptian uniform fires an automatic Kalashnikov submachine gun into a military parade reviewing stand during an attack that took the life of Egyptian President Anwar Sadat and five others at a Cairo suburb in 1981. AP/WIDE WORLD PHOTOS.



U.S. Special Forces assigned to guard Afghan President Hamid Karzai look for targets after an assassination attempt on Karzai as he was leaving the former governor's mansion in September, 2002. AP/WIDE WORLD PHOTOS.

still bears the name of his dynasty, commenced the building of the Great Wall, and established an empire that would continue for more than two thousand years.

**The cult of the Assassins.** Assassinations continued throughout the Middle Ages in western Europe and the Byzantine empire, as well as in the Muslim caliphates. It was in the Islamic world, in fact, that the first true assassins appeared on the stage. The Crusades created the political framework in which the cult of the Assassins, led by the Iranian Ismaili Hassan-i-Sabah, gained their infamous reputation, but Hassan founded the sect in 1090, a decade before the first crusaders arrived in the Holy Land, and throughout their existence, the Assassins were more apt to target Seljuk Turkish leaders than Christian invaders.

Two centuries later, Marco Polo, known for his tendency to weave fantastic tales, created a legend still believed by many today. According to Marco, Assassin leaders would ensure their men's loyalty by drugging them and taking them to a garden where they could enjoy all manner of earthly delights—pleasures which, they were told, would await them in the afterlife if they died on the field of battle. Contemporary Ismaili sources, however,

contain no mention of the "Garden of Paradise." On the other hand, it is true that the word *assassin* comes from *hashshash*, or "one who chews hashish"—a reference to the Assassins' use of the drug.

Hassan was known as the "Old Man of the Mountain," a title that passed to each successive Assassin leader. Operating from a castle in a valley stronghold, the Assassins conducted acts of terrorism and political killing throughout the Muslim world, but particularly in Iran and Iraq. Because the Seljuks happened to be in power at that time, they were the primary target, and all attempts to uproot the Assassins proved fruitless. During the Crusades, Assassins in Syria terrorized both Turks and Christians, but combined attacks by the Mongols and Mamluks in the mid-1200s brought about the end of the sect.

**Assassination in modern times.** If the roster of ancient and medieval leaders killed by assassins was too lengthy to recount in any detail, such is true many times over where the modern world is concerned. Abraham Lincoln in 1865 became the first American president killed by an assassin's bullet, followed by three others: James A. Garfield in 1881, William McKinley in 1901, and John F. Kennedy in 1963. Franklin D. Roosevelt, Harry S. Truman, Gerald Ford,

and Ronald Reagan were all targets of unsuccessful assassination attempts.

The roster of political murders in the twentieth century is lengthy. The assassination of Austrian Archduke Francis Ferdinand in 1914 precipitated World War I, and the attempted assassination of Adolf Hitler by his generals 30 years later very nearly ended World War II. Not only Mohandas K. Gandhi in 1948, but Indian Prime Minister Indira Gandhi (no relation) in 1984, and her son and successor, Rajiv Gandhi in 1991, fell victim to assassins' bullets. Leaders on both sides in the Middle East have been killed by assassins: King Abdullah of Jordan in 1951, President Anwar Sadat of Egypt in 1981, and Israeli Prime Minister Yitzhak Rabin in 1995. Interestingly, each of these leaders was killed by extremists on their own political side. On the other hand, extremist leaders are as likely as any to become targets of assassins. Senator Huey Long of Louisiana in the 1930s, and Malcolm X 30 years later, both fell to assassins' bullets. So too did George Lincoln Rockwell, leader of the American Nazi Party, and Pim Fortuyn, founder of a radical anti-immigrant party that stunned the Dutch electorate by finishing second in the 2002 parliamentary elections.

Targets of assassination are not necessarily national leaders, formal office-holders, or even political leaders. When a Turkish assassin attempted to shoot Pope John Paul II in 1981, it was clearly a political act even though the pope is not a political leader per se. Martin Luther King and Robert Kennedy, both assassinated in 1968, were political leaders, but King held no formal office and Kennedy, although he was a senator and presidential candidate, symbolized a larger cultural atmosphere of optimism and activism. Furthermore, his status as John F. Kennedy's brother added greatly to the symbolic impact of the event.

## Assassination by Stealth

Many of the assassinations mentioned in the preceding paragraphs were public acts, committed in crowded areas where the loud crack of a fired gun served as a signal of a murder in progress. Assassination committed by modern security organizations and other government-controlled response teams, however, is of a quite different nature. Indeed, assassination, whether undertaken by governments, nongovernmental organizations, or individuals acting alone, is most effective when performed in stealth.

Such was the case with an act of political murder that occurred at the outset of the modern era, during the French Revolution. As depicted in a famous painting by Jacques-Louis David, the radical leader Jean-Paul Marat was in one of the most vulnerable places—his bath—when young Charlotte Corday, a supporter of the opposition Girondists, caught up with him on the night of July 13, 1793. Corday entered Marat's private chambers under the pretense of being a journalist there to conduct an interview. More than two centuries later, the Muslim terrorist organization al-Qaeda used exactly the same pretext to gain an audience with Ahmad Shah Massoud. The leader

of the rebels in the Northern Alliance, and widely regarded as the most popular opposition figure in Afghanistan, Massoud posed the principal threat to the ruling Taliban, who provided asylum to al-Qaeda and its leader, Osama bin Laden. Two Arab al-Qaeda operatives, posing as journalists with a camera, met with Massoud in private on September 9, 2001—just two days before al-Qaeda launched its infamous terrorist attacks on the United States. As the interview began, their "camera" exploded, killing both Massoud and the two assassins.

**SMERSH and Trotsky.** An excellent example of stealth assassination undertaken by operatives working for a modern government was the assassination of Leon Trotsky in Mexico City in 1940. Trotsky had long been a rival of Josef Stalin, who recognized that Trotsky's role in launching the Bolshevik takeover of Russia alongside V. I. Lenin gave him much greater revolutionary legitimacy. Stalin had Trotsky exiled, but still wanted him dead. For more than a decade, agents of SMERSH (*SMERrt SHpionam* or "Death to Spies"), the KGB assassination team, tracked him.

The individual who finally gained Trotsky's confidence was Ramón Mercader, whom Trotsky granted a private interview. Unbeknownst to Trotsky, however, Mercader had been recruited by SMERSH in Spain during its civil war. Using the cover identity of Jacques Mornard, a French journalist, Mercader had gradually worked his way into Trotsky's inner circle, in part by seducing an American named Sylvia Agelof, who had close connections to the radical leader.

Mercader worked patiently, meeting Trotsky on several occasions before mentioning that he had written a paper on Trotsky's political philosophies, and wished to have the master himself read it. Undoubtedly flattered, Trotsky agreed to meet with him on August 20, 1940. On the appointed day, Mercader arrived bearing the putative manuscript—which was actually gibberish—along with the concealed tool necessary for his mission: a 13-inch dagger, a pistol, and an Alpine mountain climber's ice ax. After Trotsky began to read the manuscript and realized that it was only a prop, he looked up at his guest, whereupon Mercader split his skull with the ice ax. Trotsky did not immediately die, and prevented his bodyguards from killing Mercader because "He has a tale to tell." Within 24 hours, Trotsky was dead in a hospital room, and Jacques Mercador was in the custody of police. Mercador maintained his false identity as Mornard throughout his trial, where he claimed that he had killed because he was jealous that Sylvia had an intimate relationship with Trotsky. Sentenced in 1943, Mercador served 17 years in a Mexican prison. After his release, he went first to Prague and then to Moscow, where the Kremlin awarded him the Order of the Soviet Union.

**Wrath of God and "Black September."** Another instructive example of a government undertaking a careful and calculated plan of assassination is that of Israel in response to



the murder of 11 Israeli athletes at the 1972 Summer Olympic Games in Munich. The killing had occurred at the hands of Black September, a terrorist group established by the Palestine Liberation Organization (PLO) as a “deniable” action team—in other words, a group that could not be conclusively tied to its sponsors. In seeking to mete out justice to Black September, Israel in turn set up its own deniable counterterrorist unit, known as the Wrath of God.

Between 1972 and 1974, Wrath of God (nicknamed “Israel’s long arm”) allegedly killed more than a dozen Black September operatives. Wael Zwaiter, for instance, had the misfortune to find himself in a Rome elevator with what turned out to be two Wrath of God agents carrying .22 caliber pistols. The group killed Mahmoud Hamshari with an explosive device on a telephone in Paris, and claimed Hussein Bashir in Nicosia, Cyprus, with a bomb under his mattress. An explosion also claimed Mohammed Boudia, who, after a night with his girlfriend in her Paris flat, started his automobile, only to discover too late that it had been rigged with a car bomb.

As efficient as the Wrath of God was, it made some mistakes. In Lillehammer, Norway, in 1974, Wrath of God operatives shot a man they believed to be Ali Hassan Salameh, operations chief of Black September. In truth, he was Ahmed Bouchiki, a Moroccan waiter carrying an Algerian passport. Five years later in Beirut, the Wrath of God finally eliminated Salameh with an explosive device. In the meantime, the Lillehammer incident provoked complaints from western European nations vexed at the Israelis for using their cities as hunting grounds, and Israel agreed to shut down the Wrath of God.

**CIA.** It is a truism of historically alleged assassinations carried out by the Central Intelligence Agency (CIA), and other such organizations in the United States that the only operations of which the citizenry ever learns would be the botched ones. Such is the situation of an agency dedicated to covert action under the aegis of a government with a degree of openness before its polity—a problem with which SMERSH, for instance, did not have to contend.

The CIA has been publicly embarrassed by revelations of attempts to kill Fidel Castro by a number of fanciful means, such as poisoning his cigar. There have also been allegations that the agency either undertook or supported the assassinations and attempted assassinations of numerous world leaders from Chou En-Lai of China in the 1950s to Saddam Hussein in the 1990s.

These and other revelations, many of which emerged during the 1975–76 hearings led by Senator Frank Church (D-ID), helped bolster an atmosphere of public suspicion toward the CIA and NSA. From the 1970s onward, popular conspiracy theories emerged among the public that linked the CIA to almost every political slaying around the world, including the assassination of President Kennedy. Conspiracy theories aside, some trained CIA operatives possess extraordinary skill in assassination techniques. Some of those techniques are discussed in a CIA assassination

manual, apparently written in the 1950s and released to the public in 1997.

#### ■ FURTHER READING:

##### BOOKS:

Lentz, Harris M. *Assassins and Executions: An Encyclopedia of Political Violence, 1865–1986*. Jefferson, NC: McFarland, 1988.

McKinley, James. *Assassination in America*. New York: Harper & Row, 1977.

Sifakis, Carl. *Encyclopedia of Assassinations*. New York: Facts on File, 1991.

Spignesi, Stephen J. *In the Crosshairs: Famous Assassinations and Attempts*. New York: New Page Books, 2003.

##### ELECTRONIC:

Doyle, Kate, and Peter Kornbluh. *CIA and Assassinations: The Guatemala 1954 Documents*. George Washington University. <<http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB4/>> (January 30, 2003).

##### SEE ALSO

*Assassination Weapons, Mechanical*  
*Biochemical Assassination Weapons*  
*CIA (United States Central Intelligence Agency)*  
*Mossad*  
*Soviet Union (USSR), Intelligence and Security*

---

## Assassination Weapons, Mechanical

---

Throughout history, governments and groups have employed the tactic of assassination: a sudden, usually unexpected act of murder committed for impersonal reasons. The reasons for resorting to assassination have become perhaps a bit more complex as the balances of power have become more intricate, but not especially so. The purpose of assassination remains essentially the same as it was 4,000 years ago: to bring about political change quickly, or to remove someone considered a threat. The methods of assassination themselves, however, have changed greatly.

**Mechanical weapons contrasted with biochemical techniques.** In discussing assassination techniques, it is useful to divide these into mechanical and biochemical means. As their names imply, the first type of weapon gains its potency from its physical properties, whereas the second kills primarily through its effect on the individual’s biochemistry. Into the first category would fall the basic types



The .22 caliber revolver used by John Hinkley, Jr. in his 1981 assassination attempt against U.S. President Ronald Reagan, displayed at Hinkley's trial in 1982. AP/WIDE WORLD PHOTOS.

of weapon to be discussed here: bludgeons, knives, guns, and other firing devices.

To varying degrees, all of these use the mechanical principles of force, pressure, and momentum, which are related through various ratios involving the fundamental physical interactions of mass, length, and time. Additionally, several are variations on the three classic “simple machines” of classical mechanics: the inclined plane (knife), the lever (the firing mechanism of a pistol), and the hydraulic press (some types of firing devices other than pistols).

**Areas of overlap.** There is often considerable overlap between mechanical and biochemical assassination weapons. At the simplest level, all ultimately kill by impacting some aspect of the victim's biochemistry, if only by causing his brain or heart to shut down, thus bringing an end to the functions of the body itself. Furthermore, firearms employ chemical properties. The gunpowder in a bullet undergoes a chemical, rather than a merely physical change. A physical change, such as the freezing of water, is reversible, but once gunpowder has chemically been altered by the addition of heat and the process of combustion brought about by interaction with oxygen, it turns into

fire, smoke, and ash—and a fraction of it becomes energy—such that it can never become gunpowder again.

Another area of overlap is the use of firing devices to deploy the materials of biochemical assassination—that is, poisons. A classic example is the poison pen, most effectively employed by the Soviet KGB. Disguised as an ordinary writing pen, the device fired hydrocyanic acid in the form of gas. Another KGB pen-cum-assassination weapon fired pellets of ricin, a poison long favored by agents in the assassination squad known as SMERSH.

**SMERSH, poison pistols, and ricin.** SMERSH used variations on this technique to eliminate several Bulgarian dissidents living abroad in the 1970s. The most famous example of this occurred in London, where SMERSH caught up with journalist Georgi Markov in September 1978. As an unsuspecting Markov stood waiting in a crowd for a bus at Waterloo Bridge, a man walked past him and accidentally—or so it seemed—jabbed him in the thigh with the pointed end of his umbrella. The man apologized and walked on past. Within a few hours, Markov was dead. The man with the umbrella was a SMERSH assassin, and the pointed tip of his umbrella had fired a platinum pellet containing ricin.

So clever was this method of murder that it took some time before Western intelligence operatives realized what had happened, and arranged for Markov's body to be exhumed. Only then did they discover the pellet.

In this and other such cases, a biochemical agent actually caused death, yet the method of delivery was mechanical. In the same way, poison that passes through a syringe (a hydraulic pump) into the victim's body is a biochemical weapon delivered by mechanical means. By contrast, when the Aum Shinrikyo cult employed ricin to kill 12 commuters, and injure thousands more, in a Tokyo subway in 1995, they used it in the form of gas—an almost purely biochemical technique. Victims inhaled the gas, which went to work immediately on their systems.

**Basic types of mechanical assassination weapon.** The weapons under discussion here fall into a few broad categories: bludgeons; knives and other sharp objects; guns and other firing devices; and miscellaneous weapons. An encyclopedic treatment of such weapons would fill an entire book, especially where guns are concerned. Therefore, the focus here is confined to weapons, noted for their clever design or means of concealment that were developed by and for covert action organizations or similar groups. Even then, it is possible only to touch on a few notable examples.

Few of these weapons are known to be associated with a particular assassination, in part because most assassinations committed by covert-action organizations probably go undetected. Furthermore, the vast majority of assassinations are probably not directed against figures well known to the public at large, and therefore are likely to escape public attention. When Markov died, for instance, the people most likely to note the event were primarily in Bulgaria, where state-fed disinformation effectively covered all incriminating details regarding the cause of death.

**Bludgeons and blunt instruments.** A number of the potential assassination weapons that fall under the general heading of bludgeon are or were weapons for close combat also used in situations other than assassination missions. An example is the club-like instrument known as the cosh or blackjack, employed by the U.S. Central Intelligence Agency (CIA), the East German Stasi, and others. Though intended to stun the victim with a blow to the head, a cosh could certainly cause fatal injury if wielded with enough force. In a situation where a metal detector or other device would have revealed the presence of a gun, and where the operative was likely to be at close quarters with his victim, a cosh might well have been the weapon of choice.

In the 1950s, the CIA provided agents with an assassination manual that, due to the Freedom of Information Act, is now available to the public. In discussing blunt weapons, the author shows obvious respect for these simple tools of the trade, although he notes they "require some anatomical knowledge for effective use." The main

advantage of a common blunt instrument such as a hammer is its universal availability.

**Knives, edge weapons, and pointed instruments.** The CIA author was equally explicit in discussing ways to use edge weapons, a term encompassing not only knives, but also other sharp weapons. British special forces in World War II, for example, used the push dagger and the thrust weapon, both sharp instruments that are more like stakes or spikes than knives per se. Other British forces, serving as commandos in North Africa, employed a combination of knife and brass knuckles, by which the user could first stun the victim, then put the knife itself to work.

As with most assassination weapons, concealment is a key issue. Hence, many units responsible for special operations in World War II used thumb knives, which were so small they could only be gripped with the thumb and forefinger. Their size made them easy to hide in the user's clothing, or even in a closed hand. Also during the war, the British Special Operations Executive (SOE) designed an ingenious knife kit for the U.S. Office of Strategic Services (OSS), forerunner of the CIA. The kit, made to fold up and fit neatly in a pocket, contained a plethora of knives and sharp instruments, ranging from a tiny knife painted black (so as to be nonreflective) to a fierce-looking open-handled dagger. OSS never officially adopted the kit, but many of its agents took a liking to it, and acquired their own while undergoing training in Britain.

**Miscellaneous and hybrid devices.** There are also miscellaneous assassination devices that either combine aspects of the bludgeon and edge weapon, or use strangulation as a means of killing. A notorious example of the latter is the garrote, typically used when the killer is able to approach the victim unsuspected from the back. Consisting of two handles joined by a thin, strong wire a little longer than a man's shoulders, the garrote is a highly effective low-tech weapon. Some are even designed with blade-like edges to the wire so that they can double as saws if the user needs to escape from a jail cell.

Similar to the garrote is the device known as the Gigli saw. Named for Leonardo Gigli, a nineteenth-century Italian physician who used it in performing surgery, the Gigli consists of long thin tempered steel blades arranged in an oval shape, with finger rings at either end. Made to cut through bone, it could certainly be used as a killing instrument, though mercifully it is more well known as an escape device employed by British intelligence operatives.

An all-purpose device, combining aspects of both the bludgeon and the sharp instrument, was the Peskett close-combat weapon. Used in Allied special operations during World War II, the Peskett was a veritable warehouse of low-tech killing equipment. Its wrist strap and attaching

ring were the only innocuous aspects of the Peskett, whose ring attached it to a combination of cosh, garrote, and dagger. The cosh was a heavy weighted ball at the far end. The garrote wire, which could be pulled from (and retracted to) a hole on the side, also had a smaller weighted ball, which the killer employed as a grip when garroting a victim. Close to the ring and strap was a button by which the user released a dagger.

**Guns and other firing devices: clever concealment.** The designs of various guns, firing mechanisms, and explosive devices are often so clever that many of them sound more like something from a James Bond movie than actual weapons used by CIA, KGB, and other real covert-operations organizations. In such an environment, something as exotic as the CIA “Dear Weapon,” a 9-mm pistol used by the organization in Vietnam, seems perfectly ordinary. Also known as the “CIA zip gun,” it was made to be dropped in a styrofoam box from a plane. The pistol could be assembled in a matter of seconds with the help of an extremely simple instruction sheet, printed on moisture-resistant paper using pictograms that required no knowledge of English. The weapon stored ammunition in its grip, and looked like a water pistol—but it fired real bullets.

The Stinger (not to be confused with the surface-to-air missile of the same nickname) was a .22-caliber pistol hidden in a toothpaste tube. Developed for CIA during the Cold War, it was one of several guns designed for concealment in innocuous-looking packages. The British SOE also designed .22 caliber pistols disguised as either cigarettes or cigars. Both had a string at the end the smoker would put in his mouth, at which point the agent pulled the string with his teeth, firing the pistol.

Although the Bulgarians used KGB help in Markov’s case, they were also adept at designing assassination devices of their own. Bulgarian intelligence designed the keychain gun, which had two barrels and carried two .32 caliber bullets. The small size—about an inch wide and three inches long—was both an advantage and a disadvantage. On the negative side, the shortness of the barrel created a great deal of recoil, and the size of the weapon left little room for any muffling device that would reduce the loudness of the sound when fired. For this reason, the keychain gun was typically used only as a last resort. On the other hand, its size made it easy to conceal, and it was designed in such a way that the keychain gun could pass through airport metal detectors. Indeed, the keychain gun cannot be spoken of in the past tense: according to Interpol, Cold War versions or post-Cold War knockoffs continue to sell in eastern Europe for as little as \$20. After the September 11, 2001, terrorist attacks, United States aviation authorities warned airport screeners to look for keychain pistols.

Guns have also been concealed as flashlights, pipes, pencils, and any number of other ordinary-looking devices. A celebrated example was the lipstick pistol, or “kiss

of death.” Created by KGB for its female agents (or for male agents operating as homosexuals, or “ravens”), this weapon contained a 4.5-mm single-shot pistol encased in rubber and disguised as a tube of lipstick. To fire it, the user twisted its knurled ring a quarter-turn.

**Devices for firing poison gas.** Innocent-looking everyday objects provide an effective cover for assassination equipment of all types—not just pistols, but devices for firing poison gas as well. The KGB, which developed (or arranged for the development of) the poison pens described earlier, was especially talented in this area. At different times, KGB agents used wallets concealing gas-firing cartridges, as well as variations on the umbrella that killed Markov. One tool was made to look like a blind person’s cane. White tape concealed a triggering mechanism, but when the tape was removed, the user—who of course was a KGB operative with perfect vision—could fire poison gas from the cane’s handle.

The KGB used a cigarette case to hide a poison-pellet gun. Once the pack was opened, it would fire hollow-point weapons containing poison gas. Another such weapon concealed a gas-firing device that had to be removed before using. In 1954, KGB sent Nikolai Khokhlov to assassinate dissident Georgi Okolovich in West Germany using a cigarette-pack poison weapon. Khokhlov, however, had secretly converted to Christianity, and renounced his profession. Therefore he warned Okolovich about the plot and defected to the West, subsequently revealing information about the cigarette-case weapons.

#### ■ FURTHER READING:

##### BOOKS:

Irvin, Victor D. *Political Assassination: The Strategic Precision Weapon of Choice*. Carlisle Barracks, PA: U.S. Army War College, 2002.

Melton, H. Keith. *The Ultimate Spy Book*. New York: DK Publishing, 1996.

Minnery, John. *CIA Catalog of Clandestine Weapons, Tools, and Gadgets*. Boulder, CO: Paladin Press, 1990.

##### ELECTRONIC:

Doyle, Kate, and Peter Kornbluh. *CIA and Assassinations: The Guatemala 1954 Documents*. George Washington University. <<http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB4/>> (January 30, 2003).

International Spy Museum. <<http://www.spymuseum.org>> (January 31, 2003).

##### SEE ALSO

*Assassination*  
*Biochemical Assassination Weapons*  
*Knives*

## Asymmetric Warfare

■ K. LEE LERNER

In contrast to traditional warfare or “linear warfare,” asymmetric warfare refers to operations that do not rely on masses of troops or munitions to destroy and/or control an enemy. Asymmetric warfare most commonly refers to warfare between opponents not evenly matched where the smaller or weaker force must exploit geography, timing, surprise, or specific vulnerabilities of the larger and stronger enemy force to achieve victory.

At the tactical level, asymmetric warfare doctrine—first formally proposed by the ancient military strategist Sun Tzu—often attempts to specifically avoid a confrontation with the enemy’s strengths, preferring instead to disrupt or impair command functions (intelligence gathering and communications) or logistics (supply and medical care) so as to prevent the larger enemy from effectively bringing their larger force to bear in an effective manner.

At a strategic level, asymmetric war is designed to discourage and demoralize enemy forces and political leaders of those forces from using their greater strength.

The high effectiveness and low cost of asymmetric warfare has led to the inclusion of smaller and more agile units within large power forces that can specifically disengage from the larger force so as to allow larger force commanders to use asymmetric techniques.

Terrorist organizations have embraced many of the concepts of asymmetric warfare—particularly when planning operations against Western power forces. After the American-led invasion of Afghanistan following the September 11, 2001 terrorist attacks on the United States, enemy Taliban forces utilized local tribal forces to attack civilian populations and destroy food supply infrastructure in an attempt to create a humanitarian aid crisis that would slow Western coalition forces.

Because of the superpower status of United States, enemy small state and terrorist groups must utilize asymmetric warfare techniques to bolster hopes of achieving limited victories. For example, terrorist organizations hope to exploit the vulnerabilities of a free and open society in the United States and Europe. By attacking infrastructure and civilian populations, terrorist groups hope to cause political turmoil, dissent, and ultimately to change United States and European foreign policy without exposing themselves to the might of Western military forces.

### ■ FURTHER READING:

#### BOOKS:

Bailey, Kathleen C. *Iraq’s Asymmetric Threat to the United States and U.S. Allies*. Fairfax, VA: National Institute for Public Policy, 2001.

Rogers, Paul. *Political Violence and Asymmetric Warfare*. (U.S.-European Forum Paper) Washington, D.C.: Brookings Institution, 2001.

### SEE ALSO

*Biological Warfare*  
*Chemical Warfare*  
*Electronic Warfare*  
*Guerilla Warfare*  
*Information Warfare*  
*Terrorism, Philosophical and Ideological Origins*

## ATF (United States Bureau of Alcohol, Tobacco, and Firearms)

■ JUDSON KNIGHT

In accordance with the Homeland Security Act of 2002, on January 24, 2003, the Bureau of Alcohol, Tobacco, and Firearms (ATF or BATF) was transferred from the Department of the Treasury to the Department of Justice. There it became the Bureau of Alcohol, Tobacco, Firearms, and Explosives, but retained the initials ATF.

ATF is responsible for enforcing federal law with regard to the sale and use of alcohol, tobacco, firearms, and explosives. Although the ATF itself was created in 1972, at that time making it the youngest tax-collecting office of the Treasury Department, its roots go back to the founding days of the Republic. The order of items in its name corresponds to the order in which Treasury began to assume control over the items themselves: alcohol in the post-Revolutionary War era, tobacco around the time of the Civil War, and firearms during the Great Depression.

Alexander Hamilton, the first secretary of the Treasury, suggested that Congress impose a tax on imported spirits to pay a portion of the debt incurred in the War of Independence. Congress passed a resolution calling for such a tax, and in 1789 gave Treasury responsibility for collecting it. An act passed in 1862 created the Office of Internal Revenue, whose responsibilities included the collection of taxes on spirits and tobacco products. Renamed the Bureau of Internal Revenue (BIR) in 1877, in 1886 it established a laboratory that in time would assume responsibility for analyzing a variety of alcohol and tobacco products, as well as firearms and explosives.

Following the passage of the Eighteenth Amendment, which banned the sale, distribution, and consumption of alcohol, Treasury in 1920 established the Prohibition Unit. The deeds of “revenueurs” and “T-men” such as Eliot Ness in the years that followed would become legendary, as would the less admirable exploits of gangsters such as Al Capone. Nationwide concern over the violence



An Alcohol, Tobacco, and Firearms (ATF) agent searches for clues at a Manassas, Virginia, gas station in 2002 as part of the search for a sniper that terrorized the Washington, D.C. area. AP/WIDE WORLD PHOTOS.

associated with organized crime led to the passage of the National Firearms Act in 1934. Four years later, Congress passed the Federal Firearms Act, and BIR became responsible for collecting taxes on firearms.

After a number of changes in the section of BIR concerned with alcohol taxes, in 1940, this division became the ATU, or Alcohol Tax Unit. In 1942, Congress gave ATU responsibility for enforcing the Firearms Act.

**ATF separates from the Revenue Office.** Throughout much of the twentieth century, BIR had included a Miscellaneous Tax Unit (MTU), which had responsibility for tobacco taxes and, between 1934 and 1942, taxes on firearms. In 1952, MTU was dismantled, and its firearms and tobacco tax functions fell under ATU. At the same time, BIR received a new name, one familiar to millions of Americans today: Internal Revenue Service (IRS). ATU then came under IRS control as the Alcohol and Tobacco Tax Division, an arrangement that lasted for two decades.

In 1968, when Congress passed the Gun Control Act, the old BIR/IRS laboratory became responsible for analyzing firearms and explosives, and the Alcohol and Tobacco Tax Division became the Alcohol, Tobacco, and Firearms (ATF) Division. The 1970 passage of the Organized Crime Control Act made the role of the ATF Division more explicit, and signaled a shift away from IRS purview. On June 1, 1972, the Treasury Department issued Order No. 120-1, which separated the ATF from the IRS.

The order gave the new bureau authority not only over the three items listed in its name, but also over explosives. During the 1970s, ATF and its laboratory became involved in arson investigations, and in 1982, Congress amended Title XI of the Organized Crime Control Act to make arson a federal crime and formalize the ATF's role in investigating it.

During the 1990s and the beginning of the twenty-first century, ATF undertook a number of new efforts toward fighting and investigating crime. Among these was the Integrated Ballistic Identification System, a computerized program for matching weapons and ammunition fired from them. In the mid-1990s, after its abortive 1993 raid on a Waco, Texas, compound controlled by the Branch Davidian cult, the bureau became the focus of hostility on the part of fringe right-wing groups. By the turn of the century, ATF annually collected more than \$13 billion in revenue for the federal government.

■ FURTHER READING:

BOOKS:

Moore, Jim. *Very Special Agents: The Inside Story of America's Most Controversial Law Enforcement Agency—The Bureau of Alcohol, Tobacco, and Firearms*. Urbana: University of Illinois, 2001.

*A Report on the Bureau of Alcohol, Tobacco, and Firearms: Its History, Progress, and Programs*. Washington, D.C.: U.S. Government, 1995.

Vizzard, William J. *In the Cross Fire: A Political History of the Bureau of Alcohol, Tobacco, and Firearms*. Boulder, CO: Lynne Rienner, 1997.

ELECTRONIC:

Bureau of Alcohol, Tobacco, and Firearms. <<http://www.atf.treas.gov>> (December 30, 2002).

SEE ALSO

*Treasury Department, United States*

---

## Atmospheric Release Advisory Capability (ARAC)

---

The Atmospheric Release Advisory Capability (ARAC) is an effort through which the United States Department of Energy (DOE) monitors and predicts the release of hazardous materials into the atmosphere. The bulk of its activities takes place at the National Atmospheric Release Advisory Center (NARAC), located at the University of California's Lawrence Livermore National Laboratory. ARAC and NARAC have provided assessment on more than 100 incidents of hazardous-material release, whether accidental or intentional, involving nuclear, chemical, biological, and natural materials.

In 1973, Rudy J. Engelmann of the DOE consulted scientists at Livermore to learn if it were possible to create an integrated system for providing data on potential and ongoing atmospheric hazards. The laboratory undertook a feasibility study, and the result was the creation of ARAC a year later. ARAC and its national center, NARAC, got their first major test on March 28, 1979, after a malfunction in the nuclear power plant at Three Mile Island near Harrisburg, Pennsylvania, threatened to release radioactive materials into the atmosphere. NARAC analysis helped provide DOE with an accurate picture of radioactivity in and around the plant, and helped prevent an environmental disaster.

Seven years later, a far worse nuclear incident occurred in what is now Ukraine, then a part of the Soviet Union. On April 26, 1986, an accident at the Chernobyl nuclear reactor killed 31 workers immediately, and ultimately led to the deaths of some 10,000 people. With the Soviet government withholding information, even from its own citizens in the threatened area, the U.S. government turned to ARAC. Over the weeks that followed, the team at NARAC assisted western European U.S. allies in assessing the threat, and accurately predicted the subsequent spread of radioactive material across the northern hemisphere.

Accidental nuclear hazards are only one type of event among many for which ARAC has provided data. Other examples include the oil fires set by a retreating Iraqi army

during the final days of the Persian Gulf War in February 1991; the volcanic eruption of Mount Pinatubo in the Philippines in June of that year; a sulfuric-acid spill in Richmond, California, in 1993; the reentry of a nuclear-powered Russian spacecraft over Chile in 1996; and the Hanford wildfire in Richland, Washington, in 2000.

Though ARAC and NARAC might seem to be virtually identical, the former is an agency of DOE, while the latter supports both DOE, the Department of Defense, and other governmental organizations. Nor are its DOE responsibilities confined to the consequence-management mission of ARAC, though this is certainly a primary activity for NARAC. NARAC also supports other federal, state, and even local agencies in accordance with the Federal Radiological Emergency Response Plan and the Federal Response Plan.

## ■ FURTHER READING:

### BOOKS:

Cassaro, Edward, and Linda Lomonaco. *Operators Guide: Atmospheric Release Advisory Capability (ARAC) Site Facility*. Springfield, VA: Department of Energy, 1979.

Orphan, R. C. *A Study of Applying the Atmospheric Release Advisory Capability to Nuclear Power Plants*. Springfield, VA: Department of Energy, 1978.

### ELECTRONIC:

National Atmospheric Release Advisory Center. <<http://narac.llnl.gov/>> (January 14, 2003).

### SEE ALSO

*Chernobyl Nuclear Power Plant Accident, Detection and Monitoring*  
DOE (United States Department of Energy)  
Lawrence Livermore National Laboratory (LLNL)  
*Nuclear Detection Devices*

## Atmospheric Sampling Programs.

SEE *Environmental Measurements Laboratory*.

## Atomic Bomb.

SEE *Nuclear Weapons*.

audio frequency range—the range that can be perceived by the human ear—is an audio amplifier. All devices that transmit, record, or otherwise electronically process voice signals employ audio amplifiers. Voice-recognition or voice-synthesis systems, communications or eavesdropping devices, hearing aids, entertainment systems, talking toys, are examples of devices containing audio amplifiers.

**The need for amplification.** Acoustic or sound waves are longitudinal pressure waves (i.e., waves that cause molecules to oscillate along the wave's line of travel rather than across it) in air, water, or any other medium. A sound is said to be in the *audio* frequency range if it is not too high or low in frequency to be heard by the human ear. Audio sound waves may be converted by microphones into electrical signals for analysis, transmission, or recording. Electrical signals can also be converted by speakers into audible sound waves. Microphones and speakers are both transducers, that is, devices that convert energy from one form (e.g., electrical) into another (e.g., acoustic) or vice versa. Audio amplifiers are required with both microphones and speakers.

**Input amplification.** Amplification of the signal produced by a microphone—often termed preamplification—is necessary because the electrical signal that can be derived directly from sound waves impinging on a microphone is weak (i.e., on the order of .01 V or less; for eavesdropping applications, much less). Input signals of such low amplitude must be amplified before they can be processed in either analog or digital circuits.

In analog circuits—circuits that process smoothly-varying electrical quantities—there is always a certain amount of random electrical activity or “noise.” This noise is mixed with any information signal processed by the circuit, corrupting it. Amplifying a weak input, such as that from a microphone, before it mingles with circuit noise makes the noise problem manageable. Furthermore, all analog circuits that lack amplification (passive filters, transmission lines, etc.) experience signal loss; that is, they dissipate energy. A weak signal fed into a circuit that does not contain amplification will, therefore, quickly disappear, making amplification necessary in most analog circuits. Finally, amplification provides electronic isolation between the signal being amplified and the result of the amplification process; among other gains, this simplifies the circuit-design process.

If an audio signal is to be processed using digital circuitry (as is often the case today), a digital signal (i.e., on-off, high-low signal that can represent signal magnitudes symbolically) must be derived from the analog input. This conversion is performed by a device termed an analog-to-digital converter. For reasons ultimately deriving from the atomic properties of semiconductors, a typical analog-to-digital converter requires an analog input signal with an amplitude variation on the order of several

## Audio Amplifiers

### ■ LARRY GILMAN

Any electronic device that increases the power of an electrical signal whose vibrations are confined to the



volts. A low voltage signal must therefore usually be amplified before being digitized.

**Output amplification.** Wherever human ears are the ultimate destination of a signal it is necessary to drive a physical sound-making device at the output. Here audio amplification is needed for a reason complementary to that which applies at the input: the signal power needed to drive an output device (e.g., speaker or headphones) is greater than that conveyed by the signals processed throughout the circuitry of a typical electronic device, whether analog or digital. An audio amplifier is thus found at the output as well as at the input of almost every system handling signals in the audio range.

**Applications.** The number of audio amplifier designs that have been produced over the last century is probably in the hundreds of thousands. Such devices are a ubiquitous feature of modern life, and are found in computers, telephones, radios, high-fidelity audio systems, all military voice-communication systems, many appliances, and even toys.

Audio amplifiers can be miniaturized for placement in headsets, mobile phones. In applications where small size is at a premium, as in hearing aides and espionage applications (bugs and "wires"), they may be ultraminiaturized. At the high-power end, audio amplification drives public-address systems, speaker systems, and (potentially) weapons. Research is being conducted by several countries, including Russia and the U.S. (through its Low Collateral Damage Munitions Program), into the use of highly amplified sound as a weapon; frequencies in the infrasonic, audio, and ultrasonic ranges are all being considered for use against human beings. Though acoustic weapons are sometimes assumed to always be in the nonlethal category, sound can be irritating, painful, or fatal, depending on its intensity and on the efficiency with which its energy is coupled to the body.

Loud music has repeatedly been used as a psychological weapon in siege situations (e.g., by the U.S. Army against former Panamanian dictator Manuel Noriega in 1989, by cult leader David Koresh against police in 1993, and by Peruvian police during the hostage crisis at the Japanese Embassy in 1997) and as an instrument of torture. Specially-designed acoustic weapons can induce, among other effects, vomiting, choking, spasms, incontinence, thermal burns, intolerable sensations in the chest, injury to internal organs, and hearing damage. The latter is considered a serious drawback in antipersonnel applications, as hearing loss caused by intense sound is often partly or wholly permanent. Like laser weapons designed to blind (which have been outlawed by recent international agreement), acoustic weapons designed to deafen would violate international humanitarian law. Further, they would be vulnerable to obvious countermeasures, such as earplugs. Indeed, some scientists are skeptical about the possibility of developing reliable, affordable

weapons of any kind from sound. However, research and development are proceeding. Military and security applications of high-intensity sound currently under development in the U.S. or elsewhere include the following:

1. A device projecting "acoustic bullets," baseball-sized pulses of low-frequency (10-Hz) sound over distances of hundreds of yards, scalable in intensity from painful to lethal.
2. Multisensory grenades emitting disorienting light flashes, painfully loud sounds, and possibly disagreeable odors.
3. A ship-mounted system to disable crewmembers of nearby vessels (e.g., prior to boarding by Coast Guard personnel).
4. The "directed-stick radiator," an audio frequency, battery-powered weapon that could be clipped to a rifle. It fires acoustic bullets with a range in the tens of feet.
5. A helicopter-mounted nonlethal weapon emitting painfully loud sound in the audible range, with a reported (but unlikely) range of 1.2–6 miles (2–10 km).
6. Acoustic-beam weapons designed to cause discomfort: intended for embassy defense, denial of access to sensitive facilities, crowd control, and other miscellaneous antipersonnel uses.

It is unlikely that such devices will see widespread application or that, if they do, they will replace ordinary lethal weapons such as firearms. Due to the tendency of sound waves to diffuse with distance, the unpredictability of their effects on individual persons at sub-lethal levels, and the extremely high power requirements (megawatt range) for lethal levels, acoustic weapons are likely to remain a military curiosity. Audio amplification will thus remain ubiquitous in communications devices and rare in weaponry.

#### ■ FURTHER READING:

##### BOOKS:

Jones, Dwight V., and Richard F. Shea. *Transistor Audio Amplifiers*. New York: John Wiley & Sons, 1968.

##### PERIODICALS:

Altmann, Jürgen. "Acoustic Weapons-A Prospective Assessment." *Science and Global Security* no. 9 (2001): 165–244.

##### ELECTRONIC:

Roxana, Tiron. "Acoustic-Energy Research Hits Sour Note." *National Defense Magazine*. August 21, 2001. <<http://www.nationaldefensemagazine.org/article.cfm?id=746>> (December 13, 2002).

##### SEE ALSO

*COMINT (Communications Intelligence)*  
*Communications System, United States National*

## Aum Supreme Truth (Aum)

A cult (also known as Aum Shinrikyo and Aleph) established in 1987 by Shoko Asahara, the Aum aimed to take over Japan and then the world. Approved as a religious entity in 1989 under Japanese law, the group ran candidates in a Japanese parliamentary election in 1990. Over time, the cult began to emphasize the imminence of the end of the world, and stated that the United States would initiate Armageddon by starting World War III with Japan. The Japanese government revoked its recognition of the Aum as a religious organization in October 1995, but in 1997, a government panel decided not to invoke the Anti-Subversive Law against the group, which would have outlawed the cult. A 1999 law gave the Japanese government authorization to continue police surveillance of the group due to concerns that Aum might launch future terrorist attacks. Under the leadership of Fumihiko Joyu the Aum changed its name to Aleph in January, 2000, and claimed to have rejected the violent and apocalyptic teachings of its founder. (Joyu took formal control of the organization early in 2002 and remains its leader.)

**Organization activities.** On 20 March, 1995, Aum members simultaneously released the chemical nerve agent sarin on several Tokyo subway trains, killing 12 persons and injuring up to 6,000. The group was responsible for other mysterious chemical accidents in Japan in 1994. Its efforts to conduct attacks using biological agents have been unsuccessful. Japanese police arrested Asahara in May 1995, and he remained on trial facing charges in 13 crimes, including 7 counts of murder at the end of 2001. Legal analysts say it will take several more years to conclude the trial. Since 1997, the cult continued to recruit new members, engage in commercial enterprise, and acquire property, although it scaled back these activities significantly in 2001 in response to public outcry. The cult maintains an Internet home page. In July, 2001, Russian authorities arrested a group of Russian Aum followers who had planned to set off bombs near the Imperial Palace in Tokyo as part of an operation to free Asahara from jail and then smuggle him to Russia.

The Aum's current membership is estimated at 1,500 to 2,000. At the time of the Tokyo subway attack, the group claimed to have 9,000 members in Japan and up to 40,000 worldwide. The Aum's principal membership is located in Japan, but a residual branch comprising an unknown number of followers has surfaced in Russia.

### ■ FURTHER READING:

#### ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001, Annual Report: On the record briefing. May 21, 2002 <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

#### SEE ALSO

*Terrorism, Philosophical and Ideological Origins*  
*Terrorist and Para-State Organizations*  
*Terrorist Organization List, United States*  
*Terrorist Organizations, Freezing of Assets*

## Australia, Intelligence and Security

■ ADRIENNE WILMOTH LERNER

Australia gained its status as a British Commonwealth nation in 1901. The nation is largely autonomous, but technically under the British monarch. A 1999 national referendum sought to establish Australia as an independent republic, but Australians voted in favor of remaining part of Commonwealth.

Despite its location, Australia maintains close ties with the United States and Great Britain, joining the Allied efforts in World Wars I and II. Following the Second World War, Britain and the United States aided Australia in reconstructing and modernizing its intelligence community. Australian intelligence services flourished in the early 1950s, rapidly becoming one of the most advanced in the world. The nation's strategic location aided Cold War intelligence and security efforts by providing a regional location from which to monitor the expansion of Communism and Soviet influence in Asia. Today, Australia's strong intelligence community participates in international non-proliferation and anti-terrorism operations.

Australia's intelligence community is divided along traditional distinctions between civilian and military, domestic and foreign intelligence services. The Office of the Attorney General administers Australia's main civilian, domestic, intelligence agency, the Australian Security Intelligence Organization (ASIO). Founded in 1942 as the Allied Intelligence Bureau, the agency was key to allied intelligence and espionage efforts against Japan during World War II. Many of Australia's civilian intelligence services were disbanded after the war, but escalating Cold War tensions prompted their reinstatement in 1949. Today, the ASIO is charged with the protection of national security and focuses its operations on gathering and processing domestic intelligence. Participating in ongoing counter-intelligence operations, the ASIO and the Australian

Protective Service (APS) work to secure government computer, information, and communication systems from outside surveillance.

Though ASIO operations concentrate on broad-scale threats to national interests, duties such as the surveillance of extremist groups and crime syndicates are conducted with aid of accessory intelligence and security organizations. The ASIO works with the Australian Federal Police, the National Crime Authority (NCA), and the Australian Bureau of Criminal Intelligence (ABCI), providing information related to federal criminal investigations.

Australia's other large intelligence agency is the Australian Secret Intelligence Service (ASIS). The ASIS was formed in 1952, after United States and British intelligence proved to the Australian government that Soviet operatives had infiltrated high-levels of the national government. ASIS focuses on foreign intelligence, often joining international intelligence services in global peacekeeping, security, and intelligence operations. The agency relies on a variety of means, including human intelligence, to collect data, but is expressly barred from domestic political espionage or the use of weapons.

Within the ASIS are two important divisions, the Strategic Policy and Intelligence Branch (SPI) and the Intelligence and Counter-Terrorism Policy Section (ITC). The SPI coordinates intelligence and security policy among the nation's civilian intelligence community, sometimes working in close cooperation with military intelligence services. The ITC manages ASIS and inter-agency counter-terrorism efforts, sometimes working with foreign intelligence forces to combat global terrorist networks. Both divisions act as liaisons between the intelligence community and government officials, via the Office of National Assessments in the Office of the Prime Minister or Parliamentary oversight committees.

Australia's civilian intelligence community has undergone increasing scrutiny in the past two decades. In the 1990s, the Australian Parliament conducted a full review of the ASIS to determine its utility to the post-Cold War intelligence community. Parliament decided to keep the agency, but only after a detailed reorganization. In 1996, an Office of Inspector General was established to evaluate and report on the efficiency, ethicacy, and success of Australian intelligence operations. The Intelligence Services Act of 2001 placed ASIS under the stewardship of the Minister of Foreign Affairs and Trade. Parliament further implemented a formal oversight process to promote accountability in both the ASIS and the ASIO.

The Department of Defense oversees military and strategic intelligence forces. The Strategy and Intelligence Program (S&I) is the coordinated intelligence policy for Australia, managing the operations of a variety of agencies. The Defense Intelligence Organization (DIO) and the Defense Security Branch (DSB) are the major intelligence and security departments within the Department of Defense.

Australia maintains one of the world's strongest militaries. The Australian military community has three

branches, the Royal Australian Navy, Air Force, and Army, each with its own intelligence units. The Royal Australian Navy conducts both on and offshore communications intelligence and remote surveillance operations. The main concern of Naval intelligence is monitoring foreign intelligence in the South Pacific—Indian Ocean region, and protecting Australia's territorial waters.

Army intelligence conducts a variety of intelligence operations and maintains several intelligence forces. The central Army intelligence agencies are the Defense Intelligence Wing and the Army Intelligence Corps. The routine operations of these forces are predominately classified, and a majority of Army strategic intelligence forces is imbedded in combat units. The Army also operates Australia's primary military intelligence training school.

Australia's Air Force participates in international military operations, but is also charged with aiding the Royal Australian Navy in guarding Australia's territorial waters and expansive coastlines. A special division, the Maritime Patrol Group, assumes part of this responsibility, routinely patrolling the nation's coastal waterways and ports. The Air Force conducts aerial surveillance and remote intelligence operations both within Australia and abroad, in accordance with national and international law.

Law enforcement in Australia is predominantly exercised by the nation's seven territorial police agencies, as well as individual municipal police forces. The Australian Federal Police work with these agencies to infiltrate suspected crime syndicates and prevent drug trafficking, money laundering, counterfeiting, paramilitary activities, and other federal crimes.

In 2001, Australia's intelligence and security agencies joined the international fight against global terrorism. Australia's strategic position in the South Pacific and Indian Ocean regions facilitates work of intelligence community surveillance of extremist groups and terrorist networks in southern Asia and Indonesia. Australian intelligence closely monitors the proliferation of weapons and nuclear technology in Asia and the Indian Ocean region, sharing information it garners with its allies and the United Nations Security Council. Remaining committed to international non-proliferation efforts, Australia joined the Coalition forces in the 2003 war in Iraq, providing military, intelligence, and humanitarian support.

#### ■ FURTHER READING :

##### BOOKS:

Polmar, Norman and Thomas B. Allen. *Spy Book: The Encyclopedia of Espionage*. New York: Random House, 1997.

##### ELECTRONIC:

Australian Security Intelligence Organization. <<http://www.asio.gov.au/>> (1 April 2003).

Australian Secret Intelligence Service. <<http://www.asis.gov.au/>> (1 April 2003).

## Austria, Intelligence and Security

Following World War II, Austria faced the monumental task of restructuring its national government and intelligence forces. The Nazi government before and during the war substantially increased the nation's intelligence service, but post-war Austria sought to distance itself from the Nazi legacy. The intelligence system was reformed wholly, along with the nation's extensive police and security forces. Because of its central geographic location, post-war Austrian military intelligence agencies played a crucial role in signals intelligence during the Cold War.

Intelligence and security forces in Austria follow the traditional division between military and civilian, domestic and foreign intelligence agencies. The individual military services and the Ministry of Defense supervise military agencies; the Ministry of Interior regulates civilian intelligence agencies and police forces. The main units of the military intelligence force are the *Nachrichtendienstliche Aufklärung*, or Army Intelligence Service, and the *Nachrichtendienstliche Abwehr*, Army Counterintelligence Service. Both agencies primarily focus on external intelligence, often working with Austrian civilian and international intelligence agencies.

Austria's premier civilian intelligence agency is the *Generaldirektion für die Öffentliche Sicherheit*, or General Directorate for Public Safety. The agency coordinates domestic intelligence operations and assesses internal national security risks. The *Staatspolizei*, State Police, is the main national police force. The State Police is charged with ensuring public welfare and aiding in the protection of national interests within Austria's borders.

Proving that Austria is a pioneering nation in the widespread use of scientific forensic evidence, its civilian and military intelligence agencies created a nationwide DNA database. Austria's DNA database, the result of cooperation between the Ministry of the Interior and the Institute of Legal Medicine at the University of Innsbruck, was created in 1997. While the police and security agencies actively seek to expand the database, the Austrian government has enacted several measures to insure privacy and fairness in the use of the DNA database. The Ministry of the Interior maintains a database with personal information on each sample, while personal information is withheld from the lab that processes samples for criminal and intelligence investigations. The DNA database is controversial, but Austrian authorities claim the system aids police forces, protects citizens, and greatly improves counterintelligence operations.

Austria's domestic intelligence and security forces declared a new effort to combat money laundering and banking fraud in 2002. The country passed legislation in 2000 and 2001 permitting the continued use of limited

anonymous bank accounts. With the creation of a financial market intelligence unit, Austrian intelligence hope to closely monitor the use of such accounts to ensure that their funds were not used to support fraudulent enterprise, illegal trafficking, or terrorism.

Following the September 11, 2001 terrorist attacks on the United States, Austria joined the international coalition to fight terrorism. A member of the European Union, Austria pledged to contribute signals intelligence technology to pan-European counterterrorism measures. Austria's advanced and extensive financial intelligence network aids the discovery and seizure of funds used by terrorist cells. Along with Switzerland, Austria ferreted out nearly forty percent of all such illegal funds seized in Europe in 2001. The Austrian government created an inter-ministerial committee to oversee counterintelligence against the financing of terrorism. The committee, comprised of representatives from the Ministries of Finance, Justice, and the Interior, coordinates the combined efforts of Austria's various counterintelligence units and their cooperation with foreign intelligence agencies.

### SEE ALSO

*Counter-Intelligence*  
*European Union*

## Automated Biometric Identification System.

SEE *IDENT (Automated Biometric Identification System)*.

## Automatic Target Recognition (ATR).

SEE *Brain-Machine Interfaces*.

## Aviation Intelligence, History

■ JUDSON KNIGHT

As lengthy and complicated as any aspect of modern espionage, the history of aviation intelligence has involved the use of aircraft both as intelligence-gathering platforms and as objects of study. These two aspects of aviation intelligence are known as aerial reconnaissance and air technical intelligence, respectively. Over the decades, the United States has emerged as a leader in both regards, from the earliest studies of the British DeHaviland fighter in World War I, to investigations of Soviet MiG fighters during the Cold War. From prop planes to missiles, from rickety biplanes to modern satellites high above



From the Cuban missile crisis overflights to missions in support of United Nations weapons inspection teams in Iraq, the U-2 spy plane performs a diverse array of intelligence gathering operations. ©CORBIS SYGMA.

Earth's surface, aviation intelligence has involved a variety of tools since the time of its inception, just a few years after the birth of flight.

## History

The use of aircraft as instruments of both combat and reconnaissance began with the Italo-Turkish War of 1911–12. On October 23, 1911, the Italians first used an aircraft to conduct reconnaissance, against Turkish troops near Tripoli in what is now Libya. On November 1, the Italians again made aviation history when they conducted the first aerial bombing raid against an enemy. In 1912, during the same war, an Italian officer took the first aerial photographs of enemy forces from an airplane.

Aircraft also figured in the U.S. military action against Pancho Villa's Mexican rebels in 1911, and in the 1912–13 Balkan Wars. Yet at the beginning of World War I, the U.S. Army aeronautical division was woefully unprepared to gather intelligence in or on aircraft. To redress this shortcoming, the Army Signal Corps established an air technical intelligence (ATI) facility at McCook Field near Dayton, Ohio. There, in July 1917, they studied their first foreign aircraft, a British DeHaviland-4.

Meanwhile, in Europe, both sides in the world war conducted extensive aerial surveillance, with the Germans alone taking some 4,000 photographs a day. Despite Russian shortcomings in many aspects of military technology and tactics, Russia produced the most notable spy plane of the First World War: the Il'ya Mourometz bomber. Regarded as the world's first strategic reconnaissance aircraft, the Il'ya Mourometz was also the first operational four-engine plane, and could fly deep behind German lines at an altitude beyond the reach of what passed for anti-aircraft artillery at the time.

By 1920, the Army ATI facility in Dayton had become the Technical Data Section (TDS), which relocated in 1927 to Wright Field (today known as Wright-Patterson Air Force Base) near Riverside, Ohio. TDS studied more than 300 captured German aircraft, as well as hundreds of British, French, and Italian planes. Weapons, parachutes, and various airplane parts were also among the materials examined by TDS.

During the interwar years, the Germans perfected the airship, which offered considerable promise as a reconnaissance platform at a time when the use of aircraft for this purpose in its infancy. In fact, the *Graf Zeppelin*, most famous of the airships, would barely see service in a reconnaissance capacity during World War II, and then

## The Cold War

only in the early months of the conflict. On the other hand, as the Allies would discover after hostilities began, the Germans had studied reconnaissance aircraft, which yielded results in the high-altitude Ju (Junker) 86P and 86R, as well as the extremely durable Ju 88.

Other totalitarian powers also used the interwar years to build up their aerial capabilities. The Fascist Italians set the altitude record, and the Communist Russians the distance record, for aircraft during the 1930s, while the Nazi Germans established speed records. In 1939, more than a decade before jet aircraft came into use, the Germans even demonstrated a turbojet. Also during the 1930s, the Italians in Ethiopia, the Italians and Germans in Spain, and the Japanese in Manchuria, each gained considerable experience at aerial combat.

The most significant effort in aviation intelligence conducted by the British and French during the interwar years was a series of overflights in western Europe. French pilots conducted reconnaissance over western Germany beginning in 1936, and throughout 1939, British and French intelligence agencies sent Australian aviator Sidney Cotton on several flights over German and Italian facilities in Europe and North Africa. Using a specially modified Lockheed 12-A Super Electra, Cotton took a great number of photographs, and continued his reconnaissance missions throughout the war.

**World War II.** During World War II, the U.S. Army Air Force (established in 1941) modified a number of aircraft, including the B-17 Flying Fortress, B-24 Liberator, and P-51 Mustang, for reconnaissance missions. The United States also developed a few special photo-reconnaissance planes, primarily the F-11 and F-12. By the end of the war, the U.S. Ninth Air Force alone was flying some 600 photo reconnaissance missions a month from bases in the United Kingdom and western Europe.

Beginning with a U.S. Navy B-17 mission over the Solomon Islands in 1942, Allied forces also used aircraft to collect electronic intelligence (ELINT). These efforts continued and escalated throughout the remainder of the war.

At the same time, captured German and Japanese aircraft provided valuable material for study at Wright Field's ATI facility. Officers there learned to glean intelligence from the most seemingly innocuous details; for example, studies of ball bearings on German planes led to a number of successful bombing runs against German ball-bearing plants in 1943. Similarly, the nameplates of Japanese aircraft provided a wealth of target data on defense manufacturing plants in Japan.

Both sides used aircraft as a means of penetrating enemy territory and inserting intelligence operatives. This was an area in which the Germans particularly excelled, using captured Allied aircraft so as to appear less conspicuous as they dropped troops behind enemy lines. The Germans even developed a special three-man container for parachuting operatives and their equipment into hostile territory.

During World War II, the Army Air Force had organized the Air Documents Research Center (ARDC) in London to study literally tons of captured German technical documents. This effort, along with a similar one in the Pacific, greatly informed ATI during the early Cold War, an era in which aviation intelligence in all regards reached maturity.

Among the best-known aspects of the Cold War are the spy flights conducted by the United States against the Soviet Union and its allies using the U-2 and other craft. But this was only one aspect of aviation intelligence in the period after 1945, when the U.S. military turned its attention from the Axis powers to the Communist world.

So great was the number of aircraft populating the skies in the late 1940s that the Air Force—established by the National Security Act of 1947—established Project Sign (later named Project Grudge) to study unidentified flying objects (UFOs). These studies continued through 1969, and as documents released years later would show, there was never any credible evidence to authenticate the popular association of UFOs with extraterrestrial visitors. However, the widespread hysteria over UFOs in the early Cold War era serves to exemplify the palpable sense of external threat that characterized those years.

In September 1946, the United States conducted the first of many intelligence-gathering missions against the Soviets, in this case using a B-17 to collect ELINT from a Soviet station in the Arctic. In May 1951, the Air Force established the Air Technical Intelligence Center (ATIC), the principal military agency for ATI during the 1950s.

During the Korean War, the first major conflict using jet aircraft, ATIC personnel studied captured Soviet-built MiG-15 jets, as well as Il-10s and Yak-9s. At the same time, Allied forces flew reconnaissance using the RB-45C Tornado jet and other craft, collecting hundreds of thousands of images with an average of nearly 2,000 missions a month throughout most of the war.

Even as the jet made its debut, the U.S. military in Europe conducted reconnaissance against the Soviets using much older aerial technology, the balloon. Projects Moby Dick and Grand Union in the early 1950s, and Genetrix in the mid-1950s, proved less than successful, however. These failures helped influence the first overflights of Soviet territory, initially with the British Tornado, and later with the American U-2.

For their part, the Soviets proved highly adept at deceiving U.S. intelligence regarding their capabilities. They invited the American air attaché to the rehearsal for Soviet Armed Forces Day in 1954, at which their guest was shown what appeared to be 28 "Bison" bombers. This led to American estimates of a "bomber gap," though it would later turn out that the second wave of 14 bombers witnessed by the attaché was actually the first wave, flying back over. With the advent of the U-2, U.S. intelligence developed better estimates of Soviet bomber production, and instead of fearing a "bomber gap," U.S. leadership

projected a “missile gap.” This, too, would turn out to be a fallacy, thanks to intelligence collection efforts, as well as studies by ATIC in the 1950s.

The capture of U-2 pilot Francis Gary Powers in 1960 did not bring an end to U.S. intelligence-gathering missions. American intelligence continued to use the U-2, as well as other craft, including the SR-71 Blackbird and the A-12 Oxcart. All of these flew extensive missions over North Vietnam, North Korea, China, and the Middle East in the 1960s. Overflights of Cuba using U-2s provided intelligence critical to the resolution of the Cuban Missile Crisis in October 1962. Other important aerial reconnaissance craft used during the 1960s and beyond included the A3D Skywarrior and A3J Vigilante, both flown from aircraft carriers, the RF-4 (a reconnaissance version of the F-4 Phantom), the P-3 Orion, the C-47 and C-130, and others.

In the realm of ATI, ATIC became the Foreign Technology Division (FTD) in July 1961. FTD pioneered a number of technologies for the analysis and production of intelligence. As with ATIC, which brought its first Readix computer on line in 1955, FTD personnel made extensive use of computers such as the Photo Online System (PHOTOLS), an imagery database introduced in 1961. FTD also introduced the Central Information Reference and Control (CIRC) system, a computerized technical database, in 1963. Additionally, FTD pioneered machine translation of foreign languages in the Department of Defense. From an IBM Mark I Translating Device acquired by ATIC in 1959, FTD graduated to a Mark II, which provided word-for-word Russian translations at the rate of 5,000 words per hour, in October 1963.

## From the Late Cold War to the Present

During the late 1960s and early 1970s, FTD provided extensive support to U.S. efforts in Vietnam, including the December 1972 “Christmas bombings” of Hanoi and Haiphong. Beginning in 1969, FTD turned its attention from war to the prospect for peace, providing intelligence that greatly assisted U.S. diplomats taking part in the Strategic Arms Limitation Talks (SALT) and later the Strategic Arms Reduction Treaty (START) discussions. Throughout the era of detente that opened with these arms limitation talks, the United States continued to conduct surveillance against the Soviet Union. So, too, did the Soviets, whose acquisition of numerous allies during the 1970s gave them a number of friendly bases from which to conduct aerial reconnaissance missions.

U.S. efforts gained a massive boost with the launch of the KH-11, the first photographic satellite capable of directly transmitting images to a control base, in December 1976. The late Cold War also saw the introduction of unmanned reconnaissance vehicles, first flown by the Air Force in the 1960s. During their 1982 invasion of Lebanon, the Israelis debuted their Scout drones, and in the Persian Gulf War of 1991, the U.S. military made heavy use of the

Pioneer, modeled on the Scout. Operation Desert Storm also saw the extensive use of American aerial capabilities, including the E-2C Hawkeye, J-STARS, Skywarrior, Orion, and other craft. Behind the scenes, FTD provided the Pentagon with a veritable encyclopedia of Iraqi equipment, most of which had been produced by the soon-to-be defunct Soviet Union.

In October 1991, the Air Force established the Air Force Intelligence Command (AFIC), of which FTD became a part as the Foreign Aerospace Science and Technology Center (FASTC). Beginning in 1992, FASTC participated in the Open Skies treaty, whereby friendly nations flew observation aircraft freely over one another’s territory to collect information on military activities. FASTC operated the Open Skies Media Processing center from 1993. It also served as project manager for Red Tigress, a component of the Ballistic Missile Defense program, formerly known as the Strategic Defense Initiative. In October 1993, AFIC became the National Air Intelligence Center, which in turn merged with Air Combat Command in February 2001.

### ■ FURTHER READING:

#### BOOKS:

- Burrows, William E. *By Any Means Necessary: America’s Secret Air War in the Cold War*. New York: Farrar, Straus and Giroux, 2001.
- Kreis, John F. *Piercing the Fog: Intelligence and Army Air Forces Operations in World War II*. Washington, D.C.: Air Force History and Museums Program, 1996.
- Polmar, Norman, and Thomas B. Allen. *Spy Book: The Encyclopedia of Espionage*. New York: Random House, 1998.
- Richelson, Jeffrey T. *The U.S. Intelligence Community*, fourth edition. Boulder, CO: Westview Press, 1999.
- Stanley, Roy M. *World War II Photo Intelligence*. New York: Scribner, 1981.
- Taubman, Philip. *Secret Empire: Eisenhower, the CIA, and the Hidden Story of America’s Space Espionage*. New York: Simon & Schuster, 2003.

#### ELECTRONIC:

- U.S. Air Combat Command. <<http://www2.acc.af.mil/>> (April 13, 2003).

#### SEE ALSO

- Aircraft Carrier*  
*Air Force Intelligence, United States*  
*Ballistic Missile Defense Organization, United States*  
*Balloon Reconnaissance, History*  
*Hypersonic Aircraft*  
*J-Stars*  
*Korean War*  
*P-3 Orion Anti-Submarine Maritime Reconnaissance Aircraft*  
*Persian Gulf War*  
*Photographic Interpretation Center (NPIC), United States National*  
*Photography, High-Altitude Reconnaissance*  
*SIGINT (Signals Intelligence)*

*SR-71 Blackbird*  
*U-2 Spy Plane*  
*Unmanned Aerial Vehicles (UAVs)*

---

## Aviation Security Screeners, United States

---

Prior to the terrorist attacks of September 11, 2001, security screening at the more than 400 major commercial airports around the United States was the work of personnel employed by private firms that contracted with airlines. One outcome of the attacks was the Aviation and Transportation Security Act (ATSA), signed into law by President George W. Bush on November 19, 2001, which placed security screeners under the control of the newly created Transportation Security Administration (TSA). Early assessments of the new program were uneven, and TSA has encountered a number of challenges in what has proven to be one of the largest mobilizations of a civilian agency in U.S. history.

The fact that ATSA was written and passed just two months after the terrorist attacks serves to indicate the intensity of concern over air safety that prevailed in early fall, 2001. In fact, the bill would have passed even more quickly if it had not been for the thorny question of whether the government or private enterprise should control security screeners—and, assuming government control, whether Transportation or Justice was the department better suited for this task.

Also symptomatic of the post-September 11 atmosphere was the spirit of bipartisanship that pervaded the debate over ATSA. Arguments were as heated as ever, but instead of the usual division between Republicans and Democrats, this time the disagreement was between the House of Representatives and the Senate. All agreed that the old system of airlines hiring security screeners and baggage handlers had to be changed and that a new ticket tax would pay for the new federal service. Legislators in the House, however, maintained that the Department of Transportation should hire security contractors, whereas their counterparts in the Senate favored a situation in which the Department of Justice would oversee a program made up of government employees.

In the end, the two houses agreed on a compromise. Over the year that followed passage of the bill, screeners under the employment of the federal government would be phased in at 419 commercial hub airports nationwide. At the same time, up to five airports would participate in a trial program whereby they could use private contractors. After two years, all airports would be permitted to use private contractors under federal supervision, assuming they received approval to do so from the Department of Transportation.

As the debate took place on Capitol Hill, many supporters of free-market economics maintained that private enterprise could inevitably do a better job than government. Yet, the World Trade Center attacks had occurred when private firms were utilized at airports, and as legislators debated ATSA, two companies had already come under scrutiny for alleged violations of federal law. In one case, for instance, the Transportation Department found that a security company had failed to conduct background checks, and had hired screeners with criminal records.

As of January 2002, TSA had just 13 employees, but by November 2002, a year after the passage of ATSA, there were 47,000 newly trained federal security screeners at airports nationwide. TSA spokesman Robert Johnson compared the mobilization to the rush of enlistees that followed U.S. entry into World War II in December, 1941. Others were not as sanguine in their appraisal. Representative Harold Rogers (R-KY) maintained that the average screener at his home facility, Kentucky Bluegrass Airport in Lexington, processed just four people per hour.

There were other concerns as well. According to Transportation Department assistant inspector general for auditing Alexis Stefani, security companies had begun increasing their fees once the government, rather than airlines, was paying the bill. Some of this money went toward increasing the notoriously low pay of airport screeners, which had been about \$10,000 a year, to somewhere between \$23,600 and \$35,400. But, as one company had nearly doubled the rate it charged the government, it had increased employee pay by less than half that much.

Adding to TSA's challenges with the screener program were several legal battles. ATSA had contained a clause barring non-U.S. citizens from employment as airport security screeners, but in November, 2002—just as the newly mobilized screeners went to work—a federal judge in California found the ban on non-citizens unconstitutional. Meanwhile, the American Federation of Government Employees (AFGE), a union of government workers, had attempted to unionize security screeners, a move TSA officials blocked on grounds that a grant of collective bargaining rights to screeners could jeopardize national security. AFGE leaders vowed to continue the effort to unionize the screeners.

Beginning December 31, 2002, all checked bags were supposed to be screened for bombs, but as the deadline approached, it was clear that TSA would have difficulty meeting it. Screeners had already begun a practice of matching bags to passengers—that is, ensuring that for each name listed as the owner of the bag, there was a passenger with that name. Bag matching had been a practice on international flights since the 1980s, but many critics maintained that it would do nothing to stop suicide bombers such as those who perpetrated the September 11, 2001, attacks.

Meanwhile, confiscated items—some of them as unusual as deer antlers and rolling pins—piled up at airports. Some facilities had become so overwhelmed with surplus





A security screener uses a magnetic wand to check a passenger at Chicago's O'Hare International Airport in February, 2002. AP/WIDE WORLD PHOTOS.

items that they contracted with scrap-metal companies to haul away all the knives, scissors, and other sharp items confiscated. Passengers did not have to give up these items permanently, assuming the item was not illegal in the first place, and some airports had facilities for travelers to mail home items that they could not take on planes.

In contrast to these challenges and the dim prognoses offered by some critics, there was much about the federal screener program that pointed to success. The rockiness of its early months was considered inevitable in light of the monumental task administrators faced after September 11. Clearly, a mobilization such as the one required to federalize the screener program can only be properly evaluated after several months or years, not just a few weeks.

#### ■ FURTHER READING:

##### PERIODICALS:

Croft, John. "Air Security Bill Clears Lawmakers' Logjam." *Aviation Week & Space Technology* 155, no. 21 (November 19, 2001): 46.

Goo, Sara Kehaulani. "Security Law Called Unconstitutional." *Washington Post*. (November 16, 2002): A12.

———. "Security's Growing Leftovers: Confiscated or Forgotten Objects Piling Up at Country's Airports." *Washington Post*. (February 4, 2003): E1.

Lee, Christopher, and Sara Kehaulani Goo. "TSA Blocks Attempts to Unionize Screeners." *Washington Post*. (January 10, 2003): A19.

Miller, Leslie. "Some Airport Screeners Raise Rates." *San Diego Union-Tribune*. (August 27, 2002): A7.

———. "Deadline Met for Airport Security Screeners." *San Diego Union-Tribune*. (November 17, 2002): A2.

Wald, Matthew L. "Some Busy Airports to Miss Deadline for Scanning Bags." *New York Times*. (November 19, 2002): A23.

##### ELECTRONIC:

Transportation Security Administration. <<http://www.tsa.gov/public/>> (March 5, 2003).

##### SEE ALSO

*Air Marshals, United States*

*Civil Aviation Security, United States*

*FAA (United States Federal Aviation Administration)*

*September 11 Terrorist Attacks on the United States*

*Transportation Department, United States*



## B-2 Bomber

■ K. LEE LERNER

The United States Air Force B-2 stealth technology low-observable, strategic, long-range bomber is designed to penetrate air defense systems and destroy command, control, and air defense infrastructure during the opening days of a conflict when enemy forces and air defenses are fully operational.

A specially contoured radar absorbing skin and exhaust baffling system makes the flying wing configuration B-2 almost impossible to detect by radar and difficult to target with conventional thermal based system. The leading edges of the B-2 wings angle aft at approximately 33 degrees and trailing edge has a characteristic double “W” form. Although the B-2 does leave a weak RADAR return signature, the delay and low signal return confuse or obscure the B-2 track until it is too close to target—or has long passed the drop point.

The B-2 carries a crew of two and is equipped with an electronic flight instrumentation system (EFIS), that provides variable heads-up display of flight, engine, navigation, and weapons status.

Built by Northrop Grumman and costing more than \$2 billion per bomber, the B-2 is the world’s most expensive combat airplane.

The stealth technology requires special care, especially to preserve optimal “invisibility” to RADAR. To ensure this care, each B-2 is housed in a special climate-controlled hanger. The skin requires special treating occurring between missions to remove dirt and moisture. These special maintenance requirements meant that prior to Operation Iraqi Freedom the B-2 fleet operated exclusively out of Whiteman Air Force Base in Missouri. As a result, with mid-air refueling, B-2 crews flew 44-hour long round-trip bombing missions over Afghanistan in 2001. To increase the tempo of B-2 missions for Operation Iraqi Freedom, the air force transported (forward deployed)

special climate-controlled shelters at bases in England and at the Diego Garcia base in the Indian Ocean.

As of April 2003, the U.S. Air force had 21 operational B-2s. It made its first secret operational flight in 1989. Stealth technology made its debut during the Persian Gulf War (1990–1991) and the B-2 saw action in Kosovo and Afghanistan (Operation Enduring Freedom).

The B-2 is designed to carry satellite-guided bombs, including earth penetrating “bunker busters” that can penetrate 20 or 30 feet of dirt or concrete before detonating. During Operation Iraqi Freedom a B-2 led strike opened the war with an attempt on an Iraqi leadership bunker in Baghdad that western intelligence sources thought might contain Iraqi leader Saddam Hussein. Nearly three weeks later another B-2 dropped four GBU-37 “bunker buster” bombs on a Baghdad target that U.S. intelligence sources source identified as a possible meeting location for Hussein and/or other enemy leaders. The missions were notable because the B-2s, already flying above Baghdad air defenses, were fully integrated with ground based intelligence operations that allowed no more than 35 minutes to elapse from the generation of on-site intelligence to weapons delivery on target.

To maintain its stealth configuration, the B-2 carries all its weapons internally in two separate weapons bays. The B-2 can carry up to 40,000 lbs (18,000 kg) of weapons load, including both conventional and nuclear precision-guided bombs and missiles. Operating at altitudes near 50,000 ft, B-2’s can carry a number of conventional and nuclear weapons including, but not limited to, eight GBU-37s or 16 Joint Air to Surface Standoff Missiles (JASSM) and an undisclosed number of Joint Standoff Weapons (JSOW) and AGM-129 Advanced Cruise Missiles (with an estimated strike range of 1,500 miles).

### ■ FURTHER READING:

#### BOOKS:

Jones, Joseph. *Stealth Technology*. Blue Ridge Summit, PA: TAB Books, 1994.

## ELECTRONIC:

Air Force Technology, B-2. <<http://www.airforce-technology.com/projects/b2/>> (April 8, 2003).

## SEE ALSO

*F-117A Stealth Fighter*  
*Skunk Works*  
*SR-71 Blackbird*

---

## B-52

---

The Boeing B-52 Stratofortress is a bomber made for missions of extraordinarily long range. During the Persian Gulf War in 1991, it flew the longest strike mission in history, taking off from Barksdale Air Force Base in Louisiana, flying to Iraq and launching its cruise missiles, then returning to Barksdale 35 hours after it left—all without stopping. B-52s flew numerous sorties against a variety of targets during Operation Iraqi Freedom in 2003. First deployed in February 1955, the B-52 has proven its endurance over the years, and is expected to remain in service to the middle of the twenty-first century.

Over a period of eight years that ended in October 1962, a total of 744 B-52s were built and delivered. The only models remaining in service are B-52Hs, which are assigned to Air Force Air Combat Command and the Air Force Reserves. The H model, of which 102 were built, is made to carry as many as 20 air-launched cruise missiles.

Over the years, the B-52 has been modified to incorporate ever more advanced weaponry, as well as global positioning and electro-optical viewing systems. Heavy stores adapter make it possible to carry munitions of enormous weight. The aircraft weights 185,000 pounds (83,250 kg) empty, and can take off with a weight of 488,000 pounds (219,600 kg). It can travel 8,800 miles (14,080 km) without refueling, and aerial refueling gives it a range limited only by the needs of the mission and the crew. Its ceiling is 50,000 feet (15,151.5 m).

The same plane that bombed North Vietnam remained in service to bomb Iraq over a quarter-century later. It was also used in Operation Allied Force, the North Atlantic Treaty Organization (NATO) campaign against Serbia in 1999. Engineering analysis conducted at the end of the twentieth century indicated that the B-52 could remain in service past 2045—a full 90 years after its initial deployment.

## ■ FURTHER READING:

## BOOKS:

Boyne, Walter J. *Boeing B-52: A Documentary History*. New York: Jane's, 1982.  
 Holder, William G. *Boeing B-52 Stratofortress*. Blue Ridge Summit, PA: AERO, 1988.

Keaney, Thomas A. *Strategic Bombers and Conventional Weapons: Airpower Options*. Washington, D.C.: National Defense University Press, 1984.

Mandales, Mark David. *The Development of the B-52 and Jet Propulsion: A Case Study in Organizational Innovation*. Maxwell Air Force Base, AL: Air University Press, 1998.

## ELECTRONIC:

B-52 Stratofortress. Federation of American Scientists. <<http://www.fas.org/nuke/guide/usa/bomber/b-52.htm>> (March 8, 2003).

B-52 Stratofortress. U.S. Department of the Air Force. <[http://www.af.mil/news/factsheets/B\\_52\\_Stratofortress.html](http://www.af.mil/news/factsheets/B_52_Stratofortress.html)> (March 8, 2003).

## SEE ALSO

*Electro-Optical Intelligence*  
*GPS*  
*Night Vision Scopes*  
*Persian Gulf War*

## Bacillus Anthracis.

SEE *Anthrax*.

## Background Investigations, Non-Governmental.

SEE *Security Clearance Investigations*.

---

## Bacterial Biology

---

■ BRIAN D. HOYLE

An understanding of the fundamentals of bacterial biology is critical to bacteriologists and other forensic investigators attempting to identify potential biogenic pathogens that may be exploited as agents in biological warfare or by bioterrorists.

### Fundamentals of Bacterial Biology

Bacteria are one-celled prokaryotic organisms that lack a true nucleus (i.e., a nucleus defined by a membrane). Bacteria maintain their genetic material, deoxyribonucleic acid (DNA), in a single, circular chain. Bacteria also contain DNA in small circular molecules termed plasmids.

The Dutch merchant and amateur scientist Anton van Leeuwenhoek was the first to observe bacteria and other

microorganisms. Using single-lens microscopes of his own design, he described bacteria and other microorganisms as “animacules.”

In addition to not being contained in a membrane bound nucleus, the DNA of prokaryotes is not associated with the special chromosome proteins called histones, which are found in higher organisms. In addition, prokaryotic cells lack other membrane-bounded organelles, such as mitochondria.

Although all bacteria share certain structural, genetic, and metabolic characteristics, important biochemical differences exist among the many species of bacteria. The cytoplasm of all bacteria is enclosed within a cell membrane surrounded by a rigid cell wall whose polymers, with few exceptions, include peptidoglycans—large, structural molecules made of protein carbohydrate. Bacteria also secrete a viscous, gelatinous polymer (called the glycocalyx) on their cell surfaces. This polymer, composed either of polysaccharide, polypeptide, or both, is called a capsule when it occurs as an organized layer firmly attached to the cell wall. Capsules increase the disease-causing ability (virulence) of bacteria by inhibiting immune system cells called phagocytes from engulfing them.

The shape of bacterial cells are classified as spherical (coccus), rodlike (bacillus), spiral (spirochete), helical (spirilla) and comma-shaped (vibrio). Many bacilli and vibrio bacteria have whiplike appendages (called flagella) protruding from the cell surface. Flagella are composed of tight, helical rotors made of chains of globular protein called flagellin, and act as tiny propellers, making the bacteria very mobile. On the surface of some bacteria are short, hairlike, proteinaceous projections that may arise at the ends of the cell or over the entire surface. These projections, called fimbriae, facilitate bacteria adherence to surfaces.

Other proteinaceous projections, called pili, occur singly or in pairs, and join pairs of bacteria together, facilitating transfer of DNA between them.

During periods of harsh environmental conditions some bacteria can produce within themselves a dehydrated, thick-walled endospore. These endospores can survive extreme temperatures, dryness, and exposure to many toxic chemicals and to radiation. Endospores can remain dormant for long periods (hundreds of years in some cases) before being reactivated by the return of favorable conditions.

## Identifying and Classifying Bacteria

The identification schemes of *Bergey's Manual* are based on morphology (e.g., coccus, bacillus), staining (gram-positive or negative), cell wall composition (e.g., presence or absence of peptidoglycan), oxygen requirements (e.g., aerobic, facultatively anaerobic) and biochemical tests

(e.g., in which sugars are aerobically metabolized or fermented).

Another important identification technique is based on the principles of antigenicity—the ability to stimulate the formation of antibodies by the immune system. Commercially available solutions of antibodies against specific bacteria (antisera) are used to identify unknown organisms in a procedure called a slide agglutination test. A sample of unknown bacteria in a drop of saline is mixed with antisera that has been raised against a known species of bacteria. If the antisera causes the unknown bacteria to clump (agglutinate), then the test positively identifies the bacteria as being identical to that against which the antisera was raised. The test can also be used to distinguish between strains, slightly different bacteria belonging to the same species.

Pathogens are disease-causing bacteria that release toxins or poisons that interfere with some function of the host's body.

**Aerobic and anaerobic bacteria.** Oxygen may or may not be a requirement for a particular species of bacteria, depending on the type of metabolism used to extract energy from food (aerobic or anaerobic). Obligate aerobes must have oxygen in order to live. Facultative aerobes can exist in the absence of oxygen by using fermentation or anaerobic respiration. Anaerobic respiration and fermentation occur in the absence of oxygen, and produce substantially less ATP than aerobic respiration.

During the 1860s, the French microbiologist Louis Pasteur studied fermenting bacteria. He demonstrated that fermenting bacteria could contaminate wine and beer during manufacturing, turning the alcohol produced by yeast into acetic acid (vinegar). Pasteur also showed that heating the beer and wine to kill the bacteria preserved the flavor of these beverages. The process of heating, now called pasteurization in his honor, is still used to kill bacteria in some alcoholic beverages, as well as milk.

Pasteur described the spoilage by bacteria of alcohol during fermentation as being a “disease” of wine and beer. His work was thus vital to the later idea that human diseases could also be caused by microorganisms and that heating can destroy them.

## Bacterial Growth and Division

A population of bacteria in a liquid medium is referred to as a culture. In the laboratory, where growth conditions of temperature, light intensity, and nutrients can be made ideal for the bacteria, measurements of the number of living bacteria typically reveals four stages, or phases, of growth, with respect to time. Initially, the number of bacteria in the population is low. Often the bacteria are also adapting to the environment. This represents the lag phase of growth. Depending on the health of the bacteria, the lag phase may be short or long. The latter occurs if the

bacteria are damaged or have just been recovered from deep-freeze storage.

After the lag phase, the numbers of living bacteria rapidly increases. Typically, the increase is exponential. That is, the population keeps doubling in number at the same rate. This is called the log or logarithmic phase of culture growth, and is the time when the bacteria are growing and dividing at their maximum speed.

The explosive growth of bacteria cannot continue forever in the closed conditions of a flask of growth medium. Nutrients begin to become depleted, the amount of oxygen becomes reduced, and the pH changes, and toxic waste products of metabolic activity begin to accumulate. The bacteria respond to these changes in a variety of ways to do with their structure and activity of genes. With respect to bacteria numbers, the increase in the population stops and the number of living bacteria plateaus. This plateau period is called the stationary phase. Here, the number of bacteria growing and dividing is equaled by the number of bacteria that are dying.

Finally, as conditions in the culture continue to deteriorate, the proportion of the population that is dying becomes dominant. The number of living bacteria declines sharply over time in what is called the death or decline phase.

Bacteria growing as colonies on a solid growth medium also exhibit these growth phases in different regions of a colony. For example, the bacteria buried in the oldest part of the colony are often in the stationary or death phase, while the bacteria at the periphery of the colony are in the actively-dividing *log* phase of growth.

Culturing of bacteria is possible such that fresh growth medium can be added at a rate equal to the rate at which culture is removed. The rate at which the bacteria grow is dependent on the rate of addition of the fresh medium. Bacteria can be tailored to grow relatively slow or fast and, if the set-up is carefully maintained, can be maintained for a long time.

Bacterial growth requires the presence of environmental factors. For example, if a bacterium uses organic carbon for energy and structure (chemoheterotrophic bacteria) then sources of carbon are needed. Such sources include simple sugars (glucose and fructose are two examples). Nitrogen is needed to make amino acids, proteins, lipids and other components. Sulphur and phosphorus are also needed for the manufacture of bacterial components. Other elements, such as potassium, calcium, magnesium, iron, manganese, cobalt and zinc are necessary for the functioning of enzymes and other processes.

Bacterial growth is also often sensitive to temperature. Depending on the species, bacteria exhibit a usually limited range in temperatures in which they can grow and reproduce. For example, bacteria known as mesophiles prefer temperatures from 20°–50° C (68°–122° F). Outside this range, growth and even survival is limited. Other factors, which vary depending on species, required for

growth include oxygen level, pH, osmotic pressure, light and moisture.

The events of growth and division that are apparent from measurement of the numbers of living bacteria are the manifestation of a number of molecular events. At the level of the individual bacterium, the process of growth and replication is known as binary division. Binary division occurs in stages. First, the parent bacterium grows and becomes larger. Next, the genetic material inside the bacterium uncoils from the normal helical configuration and replicates. The two copies of the genetic material migrate to either end of the bacterium. Then a cross-wall known as a septum is initiated almost precisely at the middle of the bacterium. The septum grows inward as a ring from the inner surface of the membrane. When the septum is complete, an inner wall has been formed, which divides the parent bacterium into two so-called daughter bacteria. This whole process represents the generation time.

## Bacterial Genetics

Bacteria can exchange genetic material via conjugation. Genetic recombination between bacteria (or protists) occurs via a cytoplasmic bridge between the organisms. A primitive form of exchange of genetic material between bacteria involving plasmids also can occur. Plasmids are small, circular, extrachromosomal DNA molecules that are capable of replication and are known to be capable of transferring genes among bacteria. For example, resistance plasmids carry genes for resistance to antibiotics from one bacterium to another, while other plasmids carry genes that confer pathogenicity. In addition, the transfer of genes via bacteriophages—viruses that specifically parasitize bacteria—also serves as a means of genetic recombination.

Bioengineering uses sophisticated techniques to purposely transfer DNA from one organism to another in order to give the second organism new characteristics. For example, in a process called transformation, antibiotic susceptible bacteria that are induced to absorb manipulated plasmids placed in their environment can acquire resistance to that antibiotic substance due to the new genes they have incorporated. Similarly, in a process called transfection, specially constructed viruses are used to artificially inject bioengineered DNA into bacteria, giving infected cells some new characteristic.

**Bacterial adaptation and resistance.** Evolution has driven both bacterial diversity and bacterial adaptation. Some alterations are reversible, disappearing when the particular pressure is lifted. Other alterations are maintained and can even be passed on to succeeding generations of bacteria.

The first antibiotic was discovered in 1929. Since then, a myriad of naturally occurring and chemically synthesized antibiotics have been used to control bacteria.

Introduction of an antibiotic is frequently followed by the development of resistance to the agent. Resistance is an example of the adaptation of the bacteria to the antibacterial agent.

Antibiotic resistance can develop swiftly. For example, resistance to penicillin (the first antibiotic discovered) was recognized almost immediately after introduction of the drug. As of the mid 1990s, almost 80% of all strains of *Staphylococcus aureus* were resistant to penicillin. Meanwhile, other bacteria remain susceptible to penicillin. An example is provided by Group A *Streptococcus pyogenes*, another Gram-positive bacteria.

The adaptation of bacteria to an antibacterial agent such as an antibiotic can occur in two ways. The first method is known as inherent (or natural) resistance. Gram-negative bacteria are often naturally resistant to penicillin, for example. This is because these bacteria have another outer membrane, which makes the penetration of penicillin to its target more difficult. Sometimes when bacteria acquire resistance to an antibacterial agent, the cause is a membrane alteration that has made the passage of the molecule into the cell more difficult. This is adaptation.

The second category of adaptive resistance is called acquired resistance. This resistance is almost always due to a change in the genetic make-up of the bacterial genome. Acquired resistance can occur because of mutation or as a response by the bacteria to the selective pressure imposed by the antibacterial agent. Once the genetic alteration that confers resistance is present, it can be passed on to subsequent generations. Acquired adaptation and resistance of bacteria to some clinically important antibiotics became a great problem in the last decade of the twentieth century.

Bacteria adapt to other environmental conditions as well. These include adaptations to changes in temperature, pH, concentrations of ions such as sodium, and the nature of the surrounding support. This adaptation is under tight genetic control, involving the expression of multiple genes.

Bacteria react to a sudden change in their environment by expressing or repressing the expression of a whole lot of genes. This response changes the properties of both the interior of the organism and its surface chemistry.

Another adaptation exhibited by a great many bacteria is the formation of adherent populations on solid surfaces. This mode of growth is called a biofilm; bacteria within a biofilm and bacteria found in other niches, such as in a wound where oxygen is limited, grow and divide at a far slower speed than the bacteria found in the test tube in the laboratory. Such bacteria are able to adapt to the slower growth rate, once again by changing their chemistry and gene expression pattern. When presented with more nutrients, the bacteria can often very quickly resume the rapid growth and division rate of their test tube counterparts.

A further example of adaptation is the phenomenon of chemotaxis, whereby a bacterium can sense the chemical composition of the environment and either moves toward an attractive compound or shifts direction and moves away from a compound sensed as being detrimental. Chemotaxis is controlled by more than 40 genes that code for the production of components of the flagella that propel the bacterium along, for sensory receptor proteins in the membrane, and for components that are involved in signaling a bacterium to move toward or away from a compound.

### Bacteriocidal and bacteriostatic treatment of bacteria.

Bacteriocidal is a term that refers to the treatment of a bacterium such that the organism is killed. Bacteriostatic refers to a treatment that restricts the ability of the bacterium to grow.

Bacteriocidal methods include heat, filtration, radiation, and the exposure to chemicals. The use of heat is a very popular method of sterilization in a microbiology laboratory. The dry heat of an open flame incinerates microorganisms like bacteria, fungi and yeast. The moist heat of a device like an autoclave can cause deformation of the protein constituents of the microbe, as well as causing the microbial membranes to liquefy. The effect of heat depends on the time of exposure in addition to form of heat that is supplied. For example, in an autoclave that supplies a temperature of 121° F (49.4° C), an exposure time of 15 minutes is sufficient to kill the so-called vegetative form of bacteria. However, a bacterial spore can survive this heat treatment. More prolonged exposure to the heat is necessary to ensure that the spore will not germinate into a living bacteria after autoclaving. The relationship between the temperature and the time of exposure can be computed mathematically.

A specialized form of bacteriocidal heat treatment is called pasteurization after Louis Pasteur, the inventor of the process. Pasteurization achieves total killing of the bacterial population in fluids such as milk and fruit juices without changing the taste or visual appearance of the product.

Another bacteriocidal process, albeit an indirect one, is filtration. Filtration is the physical removal of bacteria from a fluid by the passage of the fluid through the filter. The filter contains holes of a certain diameter. If the diameter is less than the smallest dimension of a bacterium, the bacterium will be retained on the surface of the filter it contacts. The filtered fluid is sterile with respect to bacteria. Filtration is indirectly bacteriocidal since the bacteria that are retained on the filter will, for a time, be alive. However, because they are also removed from their source of nutrients, the bacteria will eventually die.

Exposure to electromagnetic radiation such as ultraviolet radiation is a direct means of killing bacteria. The energy of the radiation severs the strands of deoxyribonucleic acid in many locations throughout the bacterial

genome. With only one exception, the damage is so severe that repair is impossible. The exception is the radiation resistant bacterial genus called *Deinococcus*. This genus has the ability to piece together the fragments of DNA in their original order and enzymatic stitch the pieces into a functional whole.

Exposure to chemicals can be bacteriocidal. For example, the gas ethylene oxide can sterilize objects. Solutions containing alcohol can also kill bacteria by dissolving the membrane(s) that surround the contents of the cell. Laboratory benches are routinely “swabbed” with an ethanol solution to kill bacteria that might be adhering to the bench top. Care must be taken to ensure that the alcohol is left in contact with the bacteria for a suitable time (e.g., minutes). Otherwise, bacteria might survive and can even develop resistance to the bacteriocidal agent. Other chemical means of achieving bacterial death involve the alteration of the pH, salt or sugar concentrations, and oxygen level.

Antibiotics are designed to be bacteriocidal. Penicillin and its derivatives are bacteriocidal because they act on the peptidoglycan layer of Gram-positive and Gram-negative bacteria. By preventing the assembly of the peptidoglycan, penicillin antibiotics destroy the ability of the peptidoglycan to bear the stress of osmotic pressure that acts on a bacterium. The bacterium ultimately explodes. Other antibiotics are lethal because they prevent the manufacture of DNA or protein. Unlike bacteriocidal methods such as the use of heat, bacteria are able to acquire resistance to antibiotics. Indeed, such resistance by clinically-important bacteria is a major problem in hospitals.

Bacteriostatic agents prevent the growth of bacteria. Refrigeration can be bacteriostatic for those bacteria that cannot reproduce at such low temperatures. Sometimes a bacteriostatic state is advantageous as it allows for the long-term storage of bacteria. Ultra-low temperature freezing and lyophilization (the controlled removal of water from a sample) are means of preserving bacteria. Another bacteriocidal technique is the storage of bacteria in a solution that lacks nutrients, but which can keep the bacteria alive. Various buffers kept at refrigeration temperatures can keep bacteria alive for weeks.

## Bacteria and Disease

Bacteria can multiply and cause an infection in the bloodstream. The invasion of the bloodstream by the particular type of bacteria is referred to as a bacteremia. If the invading bacteria also release toxins into the bloodstream, the malady can also be called blood poisoning or septicemia. *Staphylococcus* and *Streptococcus* are typically associated with septicemia.

The bloodstream is susceptible to invasion by bacteria that gain entry via a wound or abrasion in the protective skin overlay of the body, or as a result of another infection elsewhere in the body, or following the introduction of

bacteria during a surgical procedure or via a needle during injection of a drug.

Depending on the identity of the infecting bacterium and on the physical state of the human host (primarily with respect to the efficiency of the immune system), bacteremic infections may not produce any symptoms. However, some infections do produce symptoms, ranging from an elevated temperature, as the immune system copes with the infection, to a spread of the infection to the heart (endocarditis or pericarditis) or the covering of nerve cells (meningitis). In more rare instances, a bacteremic infection can produce a condition known as septic shock. The latter occurs when the infection overwhelms the ability of the body’s defense mechanisms to cope. Septic shock can be lethal.

Septicemic infections usually result from the spread of an established infection. Bacteremic (and septicemic) infections often arise from bacteria that are normal resident on the surface of the skin or internal surfaces, such as the intestinal tract epithelial cells. In their normal environments the bacteria are harmless and even can be beneficial. However, if they gain entry to other parts of the body, these so-called commensal bacteria can pose a health threat. The entry of these commensal bacteria into the bloodstream is a normal occurrence for most people. In the majority of people, however, the immune system is more than able to deal with the invaders. If the immune system is not functioning efficiently then the invading bacteria may be able to multiply and establish an infection. Examples of conditions that compromise the immune system are another illness (such as acquired immunodeficiency syndrome and certain types of cancer), certain medical treatments such as irradiation, and the abuse of drugs or alcohol.

Examples of bacteria that are most commonly associated with bacteremic infections are *Staphylococcus*, *Streptococcus*, *Pseudomonas*, *Haemophilus*, and *Escherichia coli*.

The generalized location of bacteremia produces generalized symptoms. These symptoms can include a fever, chills, pain in the abdomen, nausea with vomiting, and a general feeling of ill health. Not all these symptoms are present at the same time. The nonspecific nature of the symptoms may prevent a physician from suspecting bacteremia until the infection is more firmly established. Septic shock produces more drastic symptoms, including elevated rates of breathing and heartbeat, loss of consciousness and failure of organs throughout the body. The onset of septic shock can be rapid, so prompt medical attention is critical.

As with many other infections, bacteremic infections can be prevented by observance of proper hygienic procedures including hand washing, cleaning of wounds, and cleaning sites of injections to temporarily free the surface of living bacteria. The rate of bacteremic infections due to surgery is much less now than in the past, due to the

advent of sterile surgical procedures, but is still a serious concern.

Bacterial infection does not always result in disease—even if a pathogen is virulent (able to cause disease). The steps of pathogenesis (the process of causing actual disease) can depend on a number of genetic and environmental factors. In some cases, pathogenic bacteria produce toxins released extracellularly (exotoxins) that migrate from the actual site of infection to cause damage to cells in other parts of the body.

#### ■ FURTHER READING:

##### BOOKS:

- Alberts, et. al. *Molecular Biology of the Cell*, 4th ed. New York: Garland Science, 2002.
- Cullimore, Roy D. *Practical Atlas for Bacterial Determination*. Boca Raton, FL: CRC Press, 2000.
- Dyer, Betsey Dexter. *A Field Guide to Bacteria*. Ithaca, NY: Cornell University Press, 2003.
- Groisman, Eduardo A. *Principles of Bacterial Pathogenesis*. Burlington, MA: Academic Press, 2000.
- Koehler, T. M. *Anthrax*. New York: Springer Verlag, 2002.
- Walsh, Christopher. *Antibiotics: Actions, Origins, Resistance*. Washington, D.C.: American Society for Microbiology Press, 2003.

##### ELECTRONIC:

The Foundation for Bacteriology, New York University. "Virtual Museum of Bacteria" <<http://www.bacteriamuseum.org/main1.shtml>> (February 5, 2003).

##### SEE ALSO

*Biological and Toxin Weapons Convention*  
*Biological Warfare*  
*Biological Weapons, Genetic Identification*  
*Bioshield Project*  
*Bioterrorism*  
*Bioterrorism, Protective Measures*  
*Viral Biology*

## Baghdad Pact.

SEE *Cold War (1950–1972)*.

## Ballistic Fingerprints

A ballistic fingerprint is the unique pattern of markings left by a specific firearm on ammunition it has discharged. Ballistic fingerprinting efficacy as a tool of forensics is a matter of some controversy. On the one hand, many law-enforcement officials insist that ballistic fingerprints are as useful as ordinary fingerprints in linking a round of ammunition to a specific gun. On the other hand, many

advocates of gun-owners' rights maintain that these fingerprints change so much over time that they are largely useless as a means of matching a spent round to a firearm.

In 1997, the National Integrated Ballistics Identification Network, established by the Federal Bureau of Investigation and the Bureau of Alcohol, Tobacco, and Firearms, made 8,800 ballistic fingerprint matches, which resulted in the linking of 17,600 crimes. As of 2000, two states—Maryland and New York—had passed laws requiring the ballistic fingerprinting of weapons. Upon selling a firearm, a dealer was required to provide the state with a spent round from the gun, so as to establish a permanent record of the gun's ballistic fingerprint. By 2002, four other states—California, Connecticut, Massachusetts, and New Jersey—were considering ballistic fingerprinting laws of their own.

Police used ballistic fingerprints, in part, to link the shootings of numerous people in the Washington, D.C., area during the fall of 2002 to the accused "Beltway snipers," John Muhammad and John Lee Malvo. The case brought ballistic fingerprinting to national attention, but not all of that attention was positive. Gun ownership advocacy groups such as Gun Owners of America and the National Rifle Association hold that ballistic fingerprints are ineffective in solving crimes, not only because the fingerprint changes over time, but also because criminals usually steal, rather than buy, their weapons. Ballistic fingerprinting, these groups claim, is actually a subtle means of further tightening gun control.

On the other hand, criminologist Daniel W. Webster, director of the Center for Gun Policy and Research at Johns Hopkins University in Baltimore, is an advocate of ballistic fingerprints as a tool of forensics, or the application of scientific techniques to crime-solving. In *Comprehensive Ballistic Fingerprinting of New Guns*, Webster cited research showing that the majority of criminals actually obtain their firearms legally. He also noted studies suggesting that though ballistic fingerprints change over time, these changes do not prevent authorities from establishing a match between a firearm and a spent round.

#### ■ FURTHER READING:

##### BOOKS:

- Lowry, Edward D. *Interior Ballistics: How a Gun Converts Chemical Energy into Projectile Motion*. Garden City, NY: Doubleday, 1968.
- Nickell, Joe, and John F. Fischer. *Crime Science: Methods of Forensic Detection*. Lexington: University Press of Kentucky, 1999.
- Webster, Daniel W. *Comprehensive Ballistic Fingerprinting of New Guns: A Tool for Solving and Preventing Violent Crime*. Baltimore, MD: Johns Hopkins Bloomberg School of Public Health, 2002.

##### ELECTRONIC:

Gun Owners of America. "Why Ballistic Fingerprinting Is Not an Effective Crime Tool." October 2002. <<http://www.gunowners.org/fs0203.htm>> (January 14, 2003).



## SEE ALSO

*Forensic Science*

## Ballistic Missile Defense Organization, United States

■ CARYN E. NEUMANN

The Ballistic Missile Defense Organization (BMDO), the successor to the Strategic Defense Initiative Organization in the United States Department of Defense, develops systems to detect, track, and destroy ballistic missiles. Working in collaboration with all of the U.S. military departments, all federal agencies, the private sector, and major research institutions, BMDOs use the most current advanced technologies to develop layered defenses that employ complementary sensors and weapons to eliminate threatening missiles in the boost, midcourse, and terminal phases of flight.

BMDO began on May 13, 1993 in the wake of a congressional ban on the deployment of space-based weapons. The collapse of the former Soviet Union had made a global attack upon the U.S. appear much less likely and Congress sought to push the Department of Defense to update missile defense programs to address the dangers of the post-Cold War world. In this changed political climate, Secretary of Defense Les Aspin announced that former President Ronald Reagan's ten-year old Strategic Defense Initiative (popularly known as "Star Wars") would be terminated with missile defense responsibilities transferred to the newly formed BMDO. At this time Aspin also changed the missile defense priorities of the United States, ordering the BMDO to focus on theater missile defense, the protection of U.S. forces deployed overseas, as well as the guarding of allies and friends. National missile defense, the protection of the U.S. from deliberate, accidental, or unauthorized limited ballistic missile attacks, would officially become a secondary priority. At the end of the decade, priorities again shifted in response to the growing threat posed by the spread of ballistic missile technology to perceived non-deterrable countries like Iraq and North Korea. Theater missile defense and national missile defense would subsequently receive equal attention as part of an integrated system of research, development, and testing programs.

To provide defense, BMDO developed a two-tier architecture system designed to intercept missiles as far away as possible from protected areas. The system is based on a hit-to-kill technology that sends a U.S. missile to destroy an enemy missile by crashing directly into it. The upper tier, named Theater High Altitude Area Defense (THAAD), provides a wide area defense including coverage of dispersed assets and population centers. After

receiving target identification and guidance information from radar, THAAD intercepts missiles either outside the atmosphere or high in the atmosphere. If the radar and operations center determines that the target has not been destroyed, then the Theater Missile Defense-Ground Based Radar (TMD-GBR) cues a lower tier system, named Patriot PAC-3, to engage the missiles that have evaded THAAD. Patriot PAC-3, an Army-run lower-tier system established in 1999 as an upgrade of the PATRIOT system, includes radar, a communications capability, and a command and control system. Navy Area Defends (NAD), a sea-based, lower-tier system upgrade of the Aegis air defense system that is the Navy's equivalent of PAC-3, will intercept missiles aimed at naval targets.

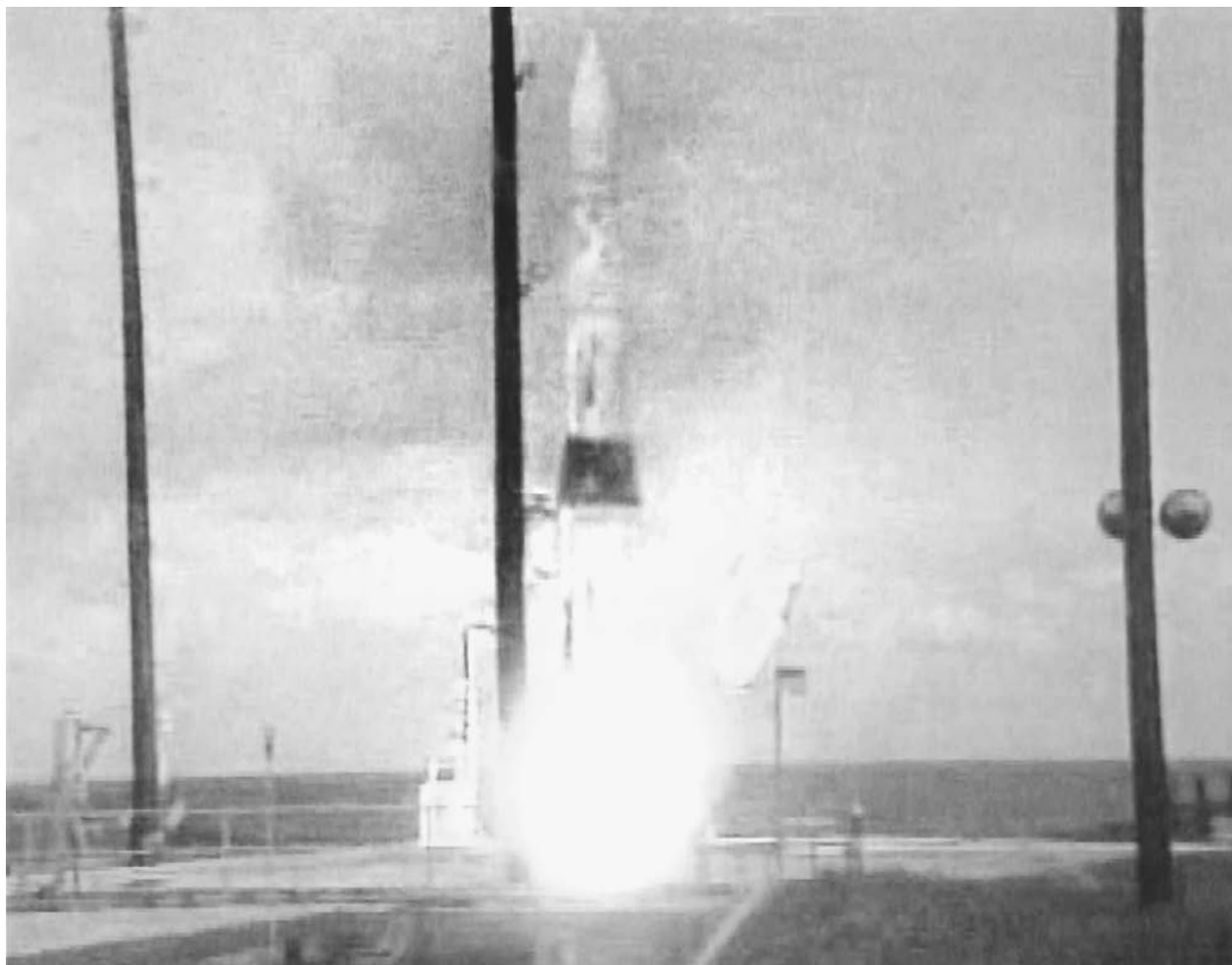
Research and testing consume the bulk of the BMDO's operating budget. It has focused on the development of kinetic and directed energy weapons such as high-energy lasers and particle-beam systems for potential sea-, ground-, air-, and space-based operations. It also bears responsibility for the creation of sensors to detect a launch, track the thruster booster of a missile through space and the atmosphere, distinguish actual warheads from decoys, and deliver this information to the battle management. It is this latter research that has been shared with the commercial scientific and technological communities. As mandated by law, the BMDO attempts to transfer its technical knowledge to U.S. companies to benefit the national economy. The BMDO Technology Applications program distributes antimissile defense technologies, such as sensors, lasers, and materials, to commercial markets in the non-defense public and private sectors.

The technology transfer program has been among the BMDO's greatest successes. The intercept of missiles with THAAD has proved enormously difficult as well as costly, but blame for the high failure rate has been placed by the Department of Defense military contractors instead of the BMDO system designers. The growing threat from foreign missiles means that the organization will likely continue to receive strong governmental support because the development of a defense system to engage all classes and ranges of ballistic missile remains an urgent need.

### ■ FURTHER READING:

#### BOOKS:

- Handberg, Roger. *Ballistic Missile Defense and the Future of American Security: Agendas, Perceptions, Technology and Policy*. Westport, CT: Praeger, 2002.
- Naveh, Ben-Zin and Azrid Lorber, eds. *Theater Ballistic Missile Defense*. Reston, VA: American Institute of Aeronautics and Astronautics, 2001.
- United States General Accounting Office National Security and International Affairs Division. *Ballistic Missile Defense: Evolution and Current Issues*. Washington, D.C.: United States General Accounting Office, 1993.
- Werrell, Kenneth P. *Hitting a Bullet with a Bullet: A History of Ballistic Missile Defense*. Maxwell AFB, AL: Air University Press, 2000.



This modified Minuteman intercontinental ballistic missile (ICBM) launched from Vandenberg Air Force Base in the U.S., was intercepted by a prototype interceptor over the Pacific Ocean in 2001. ©REUTERS NEWMEDIA INC./CORBIS.

## SEE ALSO

*Aviation Intelligence, History*  
*DOD (United States Department of Defense)*  
*RADAR*  
*Strategic Defense Initiative and National Missile Defense*

# Ballistic Missiles

■ LARRY GILMAN

Any missile that lofts an explosive payload which descends to its target as a ballistic projectile—that is, solely under the influence of gravity and air resistance—is a ballistic missile. Missiles that do not deliver a free-falling payload, such as engine powered cruise missiles (which fly to their targets as robotic airplanes), are not “ballistic.”

A ballistic missile has two basic components: a package contains guidance systems and explosives (the payload) and the rocket that lofts the payload into the upper atmosphere or into space (the booster). Ballistic missiles traverse distance rapidly; a long-range ballistic missile can travel to the other side of the world in 30 minutes. Because they give so little advance warning and deliver small, fast-moving payloads that may contain nuclear weapons capable of destroying entire cities, ballistic weapons are highly destructive and difficult to defend against.

## History

The world’s first ballistic missile was the V-2, developed by Nazi Germany during World War II. The V-2, which was first test-launched on October 3, 1942, could deliver a 1,650-lb (750-kg) warhead to a target 225 miles away. Germany launched approximately 3,000 V-2s during the war, but with little military effect; the V-2, lacking the



In 1999, Pakistan test fired this Ghauri II ballistic missile, which is capable of carrying a nuclear warhead deep inside the territory of its neighbor and rival, India.  
AP/WIDE WORLD PHOTOS.

sophisticated guidance computers of later ballistic missiles, was inaccurate. Only 50% of V-2s aimed at a given point would, on average, land within 11 mi (17 km) of that point. The V-2 was therefore not aimed at military installations but, like its predecessor the V-1 (the first cruise missile, also developed by Nazi Germany), at the city of London. Some 518 V-2s struck London during the final years of World War II, killing over 20,000 people and making the V-2 the deadliest ballistic missile in history—so far. (The “V” in V-1 and V-2 stands for *Vergeltungswaffe*, German for “retaliation weapon,” reflecting the fact that the V-2’s primary purpose was not victory but vengeance.)

The United States and Soviet Union were far behind Germany in the design of large rockets during World War II, but both captured V-2 technicians and information at the end of the war and used them to accelerate their own missile programs. The U.S. began by experimenting with captured V-2s, and during the late 1940s built several new rockets of its own based on the V-2. During the 1950s both the Soviet Union and the United States turned their attention to the development of ballistic-missile boosters that could reach the other country’s heartland from anywhere in the world. The Soviet Union flight-tested the world’s first ICBM, the R-7, in August, 1957. Two months later the R-7 was used to launch the world’s first artificial satellite, Sputnik I, and four years later launched the world’s first orbital manned space flight. The U.S. was not far behind, and by 1959 had deployed its own ICBMs, the liquid-fueled Atlas and Titan missiles. The Americans also used their ICBMs for early space-flight efforts; the first manned U.S. space flights (Mercury and Gemini programs) used the Redstone, Atlas, and Titan II missile boosters.

Throughout the Cold War, the U.S. and Soviet Union competed in the development of numerous types of ballistic missiles and built thousands of missiles in all range categories. At the peak of their buildup, which occurred in the late 1980s, the two superpowers together possessed approximately 70,000 nuclear weapons, many mounted on ballistic missiles. After the Cold War ended with the dissolution of the Soviet Union in 1991, arms-control agreements were made between Russia and the U.S. that reduced their combined nuclear arsenal to approximately 30,500 warheads. The number of ballistic missiles in all range categories was also drastically reduced.

Nevertheless, the U.S. and Russia still maintain hundreds of nuclear-armed long-range ballistic missiles (i.e., ICBMs and SLBMs) in a state of launch readiness, mostly in submarines and in concrete-lined holes in the ground (silos). Specifically, the U.S. as of 2003 has approximately 550 ICBMs carrying 2,325 warheads and 432 SLBMs carrying 3,616 warheads, while Russia (the nuclear inheritor-state of the now-dissolved Soviet Union) has approximately 756 ICBMs carrying 3800 warheads and 348 SLBMs carrying 2272 warheads. (The warhead numbers are greater than the missile numbers because of MIRVing.) The U.S. and Russia also maintain hundreds of nuclear warheads mounted on various BSRMBs, SRBMs, MRBMs, and IRBMs,

and hundreds of nuclear weapons configured for delivery by aircraft rather than by ballistic missile.

## Categories of Ballistic Missiles

With the exception of submarine-launched ballistic missiles (SLBMs), ballistic missiles are categorized according to range. Five commonly accepted categories of ballistic missile, with their associated ranges, are as follows: (1) battlefield short range ballistic missiles (BSRMBs: <93 mi [150 km]); (2) short range ballistic missiles (SRBMs: 93–497 mi [150–800 km]), (3) medium range ballistic missiles (MRBMs: 497–1490 mi [800–2400 km]), (4) intermediate range ballistic missiles (IRBMs: 1490–3416 mi [2400–5500 km]), and (5) intercontinental range ballistic missiles (ICBMs:>3416 mi [> 5500 km]).

Alternatively, the U.S. Department of Defense defines ballistic missiles with ranges less than 683 mi (1100 km) as SRBMs, those with ranges between 683 and 1708 mi (1100–2750 km) as MRBMs, those with ranges between 1708 and 3416 mi (1100–5500 km) as IRBMs.

Ballistic missiles can be launched from submarines, silos (i.e., vertical underground tubes), ships, or trailers. All ballistic missiles launched from submarines, regardless of range, are categorized as SLBMs; modern SLBMs have ranges comparable to those of ICBMs. The purpose of mounting ballistic missiles on submarines is to make them secure from attack. Modern missile submarines, such as those in the U.S. Trident class, are difficult to locate and can launch their missiles without surfacing.

## Ballistic Missile Function

The flight of a ballistic missile can be divided into three phases: boost phase, cruise phase, and descent (terminal) phase. Boost phase begins with the ignition of the missile’s booster rocket. The booster lofts the missile at a steep angle, imparting a high speed to the payload before burning out. The payload and booster then separate, beginning the cruise phase. The spent booster falls back to Earth while the payload, starting to lose speed, continues to gain altitude. If the missile is sufficiently long-range, its payload rises above the Earth’s atmosphere during cruise phase, where it jettisons its aerodynamic protective shroud and arcs under the influence of gravity. The payload may be a single cone-shaped warhead or a flat “bus” with several warheads attached to it like upside-down ice-cream cones arranged circularly on a plate.

Individual warheads are not propelled downward toward their targets on the ground, but follow ballistic paths determined by gravity and aerodynamics, gaining speed as they lose altitude. Modern reentry vehicles usually feature small external fins or other steering devices that enable them to control their course, within limits, as they fall through the atmosphere; though such maneuverable

reentry vehicles (MARVs) are not, strictly speaking, ballistic objects, missiles delivering them are still termed “ballistic” missiles for convenience. Maneuverability increases accuracy; a modern MARV delivered by ICBM or SLBM can land within a few hundred feet of its target after a journey of thousands of miles. Warheads may explode in the air high above their targets, on the surface, or under the surface after striking into the ground.

**Boosters.** The booster rockets of early ballistic missiles were powered by liquid fuels. A liquid-fuel rocket carries fuel (hydrazine, liquid hydrogen, or other) and liquid oxygen in tanks. Pressurized streams of fuel and oxygen are mixed and ignited at the top of a bell-shaped chamber: hot, expanding gases rush out of the open end of the bell, imparting momentum to the rocket in the opposite direction. Liquid fuels are unwieldy, as they must be maintained at low temperatures and may leak fuel or oxygen from tanks, pipes, valves, or pumps. Early U.S. ICBMs such as the Atlas and Titan I required several hours of above-ground preparation, including fueling, before they could be launched.

Since the late 1950s, ballistic-missile design has concentrated on solid-fuel boosters, which require less maintenance and launch preparation time and are more reliable because they contain fewer moving parts. Solid-fuel rockets contain long, hollow-core casts of a fuel mixture that, once ignited, burn from the inside out in an orderly way, forcing gases out the rear of the rocket. Starting in the early 1960s, liquid-fuel ballistic missiles were gradually phased out of the U.S. and Russian arsenals in favor of solid-fuel missiles. The first U.S. solid-fuel ICBM was the Minuteman I missile (so-called because of its near-instant response time), which was deployed to underground silos in the Midwest starting in 1962. Today, the ballistic-missile fleet of the United States consists almost entirely of solid-fuel rocket boosters. The Minuteman III, for example, like the Minuteman I and II it replaces, has a three-stage solid-fuel booster and a range of over 7000 miles. (*Stages* are independent rockets that are stacked to form a single, combined rocket. The stages are burned from the bottom up; each is dropped as it is used up, and the stage above it is ignited. The advantage of staging is that the booster lightens more rapidly as it gains speed and altitude. There are single-stage, two-stage, and three-stage ballistic missiles; the greater the number of stages, the longer the range of the missile.)

**Payloads, warheads, and MIRVs.** As mentioned above, the payload of a ballistic missile may be either a single warhead or a bus bearing several warheads which can each be sent to a different target in the same general area (e.g., the eastern United States). Such a payload is termed a *multiple independently targetable reentry vehicle* (MIRV) system, and missiles bearing multiple independently targetable warheads are said to be MIRVed. The first MIRVed missiles were deployed the U.S. in 1970; only long-range

ballistic missiles (ICBMs and SLBMs) are MIRVed. After a MIRV bus detaches from the burnt-out upper stage of its booster, it arcs through space in its cruise phase. It may possess a low-power propulsion system that enables it to impart slightly different velocities to each of its warheads, which it releases at different times. (Slight differences between individual warhead trajectories in space can translate to relatively large differences between trajectories later on, when the individual warheads are approaching their targets.) The U.S. Minuteman III ICBM is a modern MIRVed missile carrying up to three warheads; other MIRVed missiles, such as the MX, have been capable of carrying up to 10 warheads.

Regional or approximate targeting for each MIRVed warhead is achieved by bus maneuvering and release timing during cruise phase. During descent phase, the warhead may steer itself to its precise target by means of inertial guidance, radar, or a combination of the two. Inertial guidance is based on the principle that every change in an object’s velocity can be sensed by that object as an acceleration. By knowing its exact prelaunch location and state of motion (e.g., by consulting the Global Positioning System) and by precisely measuring all accelerations during and after launch, an inertial guidance system can calculate its location at all times without needing to make further observations of the outside world. Ballistic-missile payloads rely primarily on inertial guidance to strike their targets; MARVs may refine their final course by consulting the Global Positioning System (as is done, for example, by the Chinese CSS-6 SRBM) or by using radar to guide themselves during final approach (as was done, for example, by the Pershing II IRBM deployed by the U.S. in Europe during the 1980s).

The nuclear warheads mounted on modern long-range ballistic missiles are usually thermonuclear warheads having yields in the range of several hundred kilotons to several megatons. (One kiloton equals the explosive power of one thousand tons of the chemical explosive TNT; one megaton is equivalent to a million tons of TNT.) Those nations that do not possess nuclear weapons mount conventional-explosive warheads on their ballistic missiles.

**Proliferation.** Ballistic missiles offer the ability to inflict sudden damage on a distant foe. This is the central military motive behind their invention by the U.S. and Soviet Union and behind their more recent development or purchase by many states. The U.S. Department of State estimates that at least 27 nations now possess, or are in the process of developing, ballistic missiles. However, China, France, and the United Kingdom are the only countries beside the U.S. and Russia to possess *long-range* ballistic missiles (i.e., ICBMs and SLBMs): China, 20 ICBMs with 20 warheads; France, 64 SLBMs with 384 warheads; and the UK, 48 SLBMs with 185 warheads.

Of the many countries that possess some type of ballistic missile, only China, France, India, Israel, Pakistan, Russia, the United Kingdom, the United States, and (as of

early 2003) possibly North Korea have nuclear weapons to mount on them. India and Pakistan, which in the 1990s and early 2000s fought several border wars in the last few decades, are engaged in a competitive ballistic-missile development race in which India is distinctly ahead. India has produced an SRBM, the Prithvi (range 155 mi [250 km]), and an IRBM, the Agni (range 1550 mi [2,500 km]); it also has built several space-launch rockets capable of being used as ICBMs. Pakistan manufactures several BSRMBs and SRBMs of its own (the Hatf I, II, and III missiles, all with ranges of 373 mi [600 km] or less) and has purchased M-11 SRBMs from China. Israel's Jericho 2B IRBM (range 930 mi [1,500 km]) can reach southern Russia and much of the Middle East; North Korea's Taep'ong 2 IRBM (range 2,480–3,720 mi [4,000–6,000 km]) can reach much of mainland Asia, Japan, the Pacific, and probably Scandinavia. Some states (e.g., Japan, Sweden) are technically capable of building both ballistic missiles and nuclear weapons but have refrained from doing so; however, many more states are likely to develop ballistic missiles in the near future.

#### ■ FURTHER READING:

##### BOOKS:

Cimbala, Stephen J. *Nuclear Strategy in the Twenty-First Century*. Westport, CT: Praeger, 2000.

Cochran, Thomas B., William M. Arkin, and Milton M. Hoenig. *Nuclear Weapons Databook: Vol. I, U.S. Nuclear Forces and Capabilities*. Cambridge, MA: Ballinger Publishing Company, 1984.

##### ELECTRONIC:

"Ballistic Missile Threats." Centre for Defense and International Security Studies, Lancaster University, UK. Aug. 10, 2001. <<http://www.cdiss.org/bmthreat.htm>>; (March 3, 2003).

Daniel Smith. "A Brief History of 'Missiles' and Ballistic Missile Defense." Center for Defense Information. 2000. <<http://www.cdi.org/hotspots/issuebrief/ch2/>> (March 3, 2003).

##### SEE ALSO

*Ballistic Missile Defense Organization, United States Nuclear Weapons Strategic Defense Initiative and National Missile Defense*

## Balloon Reconnaissance, History

#### ■ JUDSON KNIGHT

Just three months after the first manned balloon flights in France in 1783, Benjamin Franklin wrote of the new invention's military capabilities. Over the next 13 decades,



An American major in the basket of an observation balloon flying over fields near the front lines in France, June 1918. ©CORBIS.

balloons would increasingly serve fighting forces both for reconnaissance—particularly in the American Civil War—and later as bombers. The latter application would reach its apex with the German airships of World War I, a conflict in which the airplane proved itself a vastly superior instrument of aerial combat. Thereafter, the principal nation using balloons for surveillance was not Germany, but the United States, which employed them in the Second World War. American use of surveillance balloons and blimps continued even into the Cold War and the early twenty-first century war on drugs and homeland defense efforts.

### The Principle of Buoyancy

Balloons and airplanes both rise into air, but by very different means. An airplane flies accordance to aerodynamic principles involving the relative pressure and speed of fluids (air and other gases are considered fluids in the terms of physics), and its lift depends heavily on the design of the wing's leading edge—a design borrowed from that which nature has given to the bird's wing. A balloon, on the other hand, rises according to the principal of buoyancy discovered by the Greek physicist and mathematician Archimedes (c. 287–212 B.C.)

According to Archimedes's principle, the buoyant force of an object immersed in fluid is equal to the weight of the fluid displaced by the object. This explains how a

metal aircraft carrier weighing thousands of tons can float. If all the metal were crushed into a ball, it would sink to the bottom of the ocean, but when designed properly, the area inside the hull weighs less than the water it displaces. Similarly, the gases inside the envelope of a balloon must weigh less than the air around them.

**Gases for buoyancy.** There are three gases practical for use in balloons: hydrogen, helium, and heated air. Hydrogen would be ideal, except for the fact that it is extremely flammable, and helium, which was not discovered in elemental form until the 1860s, is extremely expensive to produce. On the other hand, heated air requires only a reliable heating source.

As French chemist J. A. C. Charles, an early balloon enthusiast, recognized in his famous law of gases, heating a gas increases its volume; thus, the air molecules inside the envelope of a balloon tend to spread apart, reducing the density of the air inside and making the craft buoyant. Ironically, Charles introduced the hydrogen balloon, which would dominate until the 1937 explosion of the *Hindenburg*. Since that time, most balloons have used heated air.

**From the late eighteenth century to the U.S. Civil War (1783–1863).** French brothers Joseph-Michel and Jacques-Etienne Montgolfier launched the first balloon on June 5, 1783. Later that year, the Montgolfiers sent up the first balloon crew—a sheep, a rooster, and a duck—and on November 21, Jean-François Pilatre de Rozier became the first human being to ascend in a balloon.

The first army air corps was born in revolutionary France in 1794, when a balloon contingent was established for reconnaissance purposes. The French used balloon reconnaissance extensively in the Napoleonic wars, and by the mid-nineteenth century, Britain, Russia, Austria, and Denmark were using balloons for military purposes.

In 1849, the Austrians undertook the first aerial bombardment campaign, using 200 unpowered hot-air balloons against the Venetians. The effort proved disastrous when winds blew the balloons, whose explosives were set on timers, back to the Austrian side.

**Balloons in the early United States.** Whereas the Austrians' experience illustrated the problematic nature of balloons as bombers, the American experience in the Civil War showed that balloons had great potential for reconnaissance and purposes other than combat. For several decades, visionary military leaders had called for the use of balloons in warfare. During the Seminole War in Florida (1835–1842), Col. John Sherburne tried unsuccessfully to gain War Department support for a plan to use balloons for spotting Seminole campfires at night. A decade later, in the Mexican War, John Wise, later dubbed "the Father of American Aeronautics," proposed a balloon bombing

campaign against the city of Veracruz, although the War Department ignored his proposal.

During the Civil War, Wise was one of several who proposed the use of balloon reconnaissance by the Union, but by far the most successful promoter of balloon reconnaissance was Thaddeus Lowe. While attempting unsuccessfully to cross the Atlantic by balloon, Lowe had found himself behind Confederate lines at the outset of the war, in April 1861. Having observed some military activity, Lowe offered his services to Union leadership, and proved to be the only balloonist the Union seriously considered. On June 17, 1861, Lowe and a telegraph officer ascended 500 feet (152 m) above the Columbia Armory in Washington, with telegraph lines running along the rigging wires and connecting them to the War Department and White House. Lowe's efforts won the support of President Abraham Lincoln, and over the next two years, the Union Army became host to one of the war's great experiments in technology and intelligence.

**The Union balloon corps.** During the winter of 1861–1862, Lowe gathered around himself an aeronautic crew that included two other ballooning pioneers, brothers Ezra and James Allen. They developed a system of signals from the ground to the air, and a method for getting balloons aloft while avoiding trees. They also found an effective means of transporting balloons, primarily aboard barges. While aloft, aeronauts, sometimes accompanied by military observers, would study details ranging from dust clouds to campfires, counting or if necessary merely estimating the number of enemy troops they saw. With a telescope, they could see as far as 30 miles (48 km) on a clear day.

The Confederates' many attempts to shoot down Lowe's balloons, which earned him the title "most shot-at man in the war," illustrated the effect the balloons had on morale. Years later, Confederate artillery officer E. P. Alexander said, "I never understood why the enemy abandoned the use of military balloons.... Even if the observers never saw anything, they would have been worth all they cost for the annoyance and delays they caused us in trying to keep our movement out of sight." The Southern states attempted to field their own balloons, but in this as in other areas, they lacked the technological means to effectively challenge the North. They finally did send up a balloon, made from silk dresses, but the Union promptly captured it.

Although Lowe's corps had the technological advantage over the enemy, the Union ballooning effort was doomed. Most Union generals failed to see the balloon's usefulness for a reconnaissance, and the fact that Lowe and his crew were civilians only added to the War Department view of them as outsiders. Lowe resigned in April 1863, and although the Allen brothers kept the balloons aloft for a few months, the corps had faded away by that summer. One of their last intelligence reports was of Confederate troops moving from Fredericksburg, Virginia,

toward the Blue Ridge Mountains, the opening movements of a campaign that would lead to the decisive battle at Gettysburg, Pennsylvania.

## From the Franco-Prussian War to World War I (1870–1918)

Balloons again proved their effectiveness for the French during the siege of Paris in 1870, when 66 balloons managed to transport 102 people and more than 2 million pieces of mail past the Germans. Impressed, the Germans formed their own balloon corps in 1884, and the Austrians in 1893. Russia opened a school of aeronautic training outside St. Petersburg. Britain, meanwhile, began military balloon training in 1880.

Still, the experience of the French in 1870 illustrated the limits of balloons. First, they could not be steered, and could only go with the wind. Second, the Prussians were rumored to have developed anti-aircraft guns that could shoot them down—which, while not true at the time, boded ill for low-flying craft.

**Rise of the airship.** By that time, a new variation on the old-fashioned envelope-and-gondola balloon had begun to show promise. This was the airship, an idea whose origins dated back to the Montgolfiers' era. Around the same time as the first balloon launches, another French designer, Jean-Baptiste-Marie Meusnier, began experimenting with a more streamlined, maneuverable model.

It was more than a century before Meusnier's idea became a reality. In 1898, Alberto Santos-Dumont of Brazil combined a balloon with a propeller powered by an internal-combustion engine. Although these men more clearly qualify as the fathers of the airship, they were to be eclipsed in history by a figure whose name became a synonym for it: Germany's Count Ferdinand von Zeppelin.

**The Zeppelin.** Zeppelin created a lightweight structure of aluminum girders and rings that made it possible for an airship to remain rigid under varying atmospheric conditions. The Zeppelins of World War I were legendary, as terrifying to the enemy as they were inspiring to Germans who sent them aloft.

At first, the German army failed to grasp their potential, so the navy began using them to scout British cruisers in the North Sea. At a time when aircraft were still in their infancy, and when the British fleet used light cruisers for reconnaissance at sea, the Zeppelin was both safer than an airplane and vastly more economical than a cruiser. In 1914, Zeppelin's company was turning out three airships a year; two years later, it was producing more than two a month.

Along the way, the use of Zeppelins as bombers overshadowed their role as reconnaissance craft. In 1915—fully a quarter-century before the Nazis' more famous

bombardment—the Germans launched the first air battle of Britain. Far beyond the actual physical damage the Zeppelins wrought was the psychological effect of the dark shapes appearing in the British sky. At 10,000 feet (3,048 m), they were too high for antiaircraft guns of the time to reach them, and therefore they rained terror at will.

Even so, Zeppelins were cumbersome, dangerous craft, and in the final analysis, they were not cost-effective either for reconnaissance or for bombing. By September, 1916, the British had at their disposal explosive bullets that, when fired from an airplane, could shoot Zeppelins from the sky. Even the psychological value of Zeppelins proved a double-edged sword: recruiting posters and anti-German propaganda made heavy use of the Zeppelin as a symbol of the enemy.

## Balloons from the 1920s to the Present

For a few years after war's end, airships constituted the luxury liners of the skies, but the *Hindenburg* crash signaled the end of relatively widespread airship transport. In the meantime, the U.S. Navy had taken an interest in airships, several of which were built for it by the Goodyear Tire and Rubber Company during the 1920s and early 1930s. After several mishaps involving rigid airships, the navy switched entirely to nonrigid airships, or blimps.

During World War II, the U.S. Navy was to be the only fighting force on either side to use airships. After the attack on Pearl Harbor, Congress authorized the construction of some 200 airships, which the navy used for photographic reconnaissance, scouting, minesweeping, antisubmarine patrols, search and rescue, and escorting convoys. Some 89,000 ships were escorted by airships during the war, and not a single one was lost. Although they were slow compared to airplanes, balloons could stay aloft for as much 60 hours, a decided advantage in an era before in-flight refueling.

Non-reconnaissance uses of balloons during the war included their employment by the British as protection against bombers, which had to fly over them to avoid their mooring wires, thus placing the Luftwaffe further from their targets and impairing accuracy. The Japanese employed some 1,000 "Fu-Go Weapons," or balloons equipped with bombs, which they sent eastward across the Pacific. These landed in some 16 U.S. states, as well as in Alaska, Canada, and Mexico. They killed only six civilians—a mother and her five children in Lakeview, Oregon, in May 1945—and the fact that the U.S. media agreed not to report news of the bombings greatly blunted their potential psychological effect.

**The Cold War: Project GENETRIX.** By far, the most significant use of balloon reconnaissance during the Cold War was Project GENETRIX. The program had its origins in a 1951 study by the RAND corporation, and in December 1955,



President Dwight D. Eisenhower gave approval for the U.S. Air Force to launch 516 camera-carrying balloons over Eastern Europe, the Soviet Union, and the People's Republic of China.

GENETRIX proved a disaster in several regards. Only 34 balloons—about 7% of the total—survived and produced usable, useful images. Worse than the poor return ratio was the public-relations opportunity that the project provided to the communist bloc, which protested U.S. spying and used information on GENETRIX for propaganda purposes.

Central Intelligence Agency (CIA) officials called on the air force to halt GENETRIX, which it did in February 1956. At the time, the CIA was planning the launch of U-2 overflights, and they feared that GENETRIX would turn Eisenhower against the concept of overflights. Additionally, they were concerned that the program might negatively affect an effort by the Free Europe Committee, a CIA front based in West Germany, to drop propaganda leaflets over Eastern Europe.

The failure of GENETRIX concealed several successes. The images of the Soviet Union it did produce provided the best available record between World War II and the advent of the U-2 reconnaissance plane and later satellites. Additionally, the high-flying balloons, which averaged an altitude of 45,800 feet (13,960 m), provided data on wind currents that helped scientists determine the best flight paths for the U-2.

Finally, the most curious benefit of GENETRIX was the fact that a steel bar that secured the envelope, cameras, and ballasting equipment happened to measure 2.99 feet (91 cm)—exactly the same size as the wavelength of Soviet radar known as TOKEN to NATO (North Atlantic Treaty Organization) forces. Because it resonated when TOKEN pulses hit it, the bar helped NATO radar operators locate previously unknown radar installations. This, too, aided the U-2 project.

**Balloon reconnaissance today.** The navy, which had continued its balloon program until 1962, attempted to revive it in the 1980s, but Congress cut off all funding in 1989. Yet, the usefulness of balloons and blimps for surveillance is far from exhausted. Their virtual invisibility with regard to radar has reinvigorated interest in blimps on the part of the U.S. Department of Defense, which has discussed plans to use airships as radar platforms in a larger Strategic Air Initiative.

Meanwhile, the air force employs aerostats, or unmanned, aerodynamically shaped blimps tethered by a single cable, in its Tethered Aerostat Radar System, a counter-narcotics surveillance program along the U.S.-Mexico border. Aerostats offer a number of advantages, including enormous detection range and coverage. Typically occupying an altitude of about 15,000 feet (4,500 m), an aerostat can cover 185 square miles (480 sq km) and track smaller, lower-flying aircraft such as those used by

drug smugglers. They can operate virtually without break at low cost, and need come down only for routine maintenance and severe weather. It is calculated that an aerostat can provide surveillance at a cost about 5% as great as that of an airplane. Kept aloft by helium, a highly non-reactive gas, they also have a considerably accident free record of operation.

#### ■ FURTHER READING:

##### BOOKS:

- Brugioni, Dino A. *From Balloons to Blackbirds: Reconnaissance, Surveillance, and Imagery Intelligence: How It Evolved*. McLean, VA: Association of Former Intelligence Officers, 1993.
- Evans, Charles M. *The War of the Aeronauts: A History of Ballooning during the Civil War*. Mechanicsburg, PA: Stackpole Books, 2002.
- Lebow, Eileen F. *A Grandstand Seat: The American Balloon Service in World War I*. Westport, CT: Praeger, 1998.
- Peebles, Curtis. *The Moby Dick Project: Reconnaissance Balloons over Russia*. Washington, D.C.: Smithsonian Institution Press, 1991.

##### PERIODICALS:

- Fanton, Ben. "View from above the Battlefield." *America's Civil War* 14, no. 4 (September 2001): 22–28.
- Nahum, Hazi, and Sheike Marom. "Aerostat-Borne Systems for Defense and Homeland Security." *Military Technology* 26, no. 8 (August 2002): 102–108.

##### ELECTRONIC:

- U.S. Centennial of Flight. <<http://www.centennialofflight.gov>> (March 13, 2003).

##### SEE ALSO

- Civil War, Espionage and Intelligence*  
*Reconnaissance*  
*U-2 Spy Plane*  
*World War I*

---

## Basque Fatherland and Liberty (ETA)

---

The ETA was founded in 1959 with the aim of establishing an independent homeland based on Marxist principles in the northern Spanish Provinces of Vizcaya, Guipuzcoa, Alava, and Navarra, and the southwestern French Departments of Labourd, Basse-Navarra, and Soule. The Basque Fatherland and Liberty (ETA) group also operates as, or is known as Euzkadi Ta Askatasuna.

**Organization activities.** The ETA is primarily involved in bombings and assassinations of Spanish government officials, security and military forces, politicians, and judicial figures. ETA finances its activities through kidnappings, robberies, and extortion. The group has killed more than 800 persons and injured hundreds of others since it began lethal attacks in the early 1960s. In November 1999, ETA broke its “unilateral and indefinite” cease-fire and began an assassination and bombing campaign that had killed 38 individuals and wounded scores more by the end of 2001.

The actual size of ETA is unknown, but estimates indicate that ETA may have hundreds of members, plus supporters. The ETA operates primarily in the Basque autonomous regions of northern Spain and southwestern France, but also has bombed Spanish and French interests elsewhere.

ETA members have received training at various times in Libya, Lebanon, and Nicaragua. Some ETA members allegedly have received sanctuary in Cuba while others reside in South America.

#### ■ FURTHER READING:

##### ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001, Annual Report: On the record briefing. May 21, 2002 <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

##### SEE ALSO

*Terrorism, Philosophical and Ideological Origins*  
*Terrorist and Para-State Organizations*  
*Terrorist Organization List, United States*  
*Terrorist Organizations, Freezing of Assets*

## Bathymetric Maps

#### ■ ALEXANDR IOFFE

Bathymetric mapping refers to construction of ocean and sea maps—bathymetric maps (BM). Bathymetric maps represent the ocean (sea) depth depending on geographical coordinates, just as topographic maps represent the altitude of Earth’s surface at different geographic points. Bathymetric maps are critical to submarine navigation, submarine evasion tactics, and in predicting the location of ocean signal channels.

The most popular kind of bathymetric maps is one on which lines of equal depths (isobaths) are represented. Like geographical maps of the surface of Earth, bathymetric maps are constructed in definite cartography projection. Mercator projection is used perhaps more often in constructing bathymetric maps, and has been used for a long time in constructing sea charts that are used for sailing in all latitudes except Polar ones.

The creation of a bathymetric map of a given region depends above all on the amount of depth measurement data for that region. Before the invention of the echosounder in the 1920s, ocean (sea) depth could be measured only by lead. Such measurements were quite rare; these measurements were made only in isolated points, and creation of bathymetric mapping was practically impossible. Thus, the structure of the ocean floor was virtually unknown. It should be noted, for example, that the most important structure in the Atlantic Ocean, the Middle-Atlantic ridge, was discovered and began to be investigated only after World War II. Another important factor for creating bathymetric mapping is determining geographical coordinates of the point where the depth measurement is made. It is evident that when these determinations are more precise, then the maps are better. As of 2003, the GPS (Global Positioning System) is used for determining the coordinates of the measurement points.

When constructing topographic maps of land, one can always measure the altitude of any point of the surface precisely. However, when constructing a bathymetric map, it is practically impossible to determine the exact depth of any point of the bottom of the sea. Obviously, bathymetric maps are more precise when more data of depth measurement per surface area unit in the given region are available. Currently, the most precise and detailed bathymetric maps result from using data from multibeam echosounding. The multibeam echosounder is a special kind of echosounder, which is located on board of the vessel and measures the depth simultaneously in several points of the bottom. These points are located on the straight line perpendicular to the vessel track. These points themselves are determined by the reflection of several acoustical pulses (beams) directed from one point at different angles to the vertical. The determination of depth in this method is performed regularly within periods of several seconds during the vessel motion. The measurement data are stored in a computer, and using them the map of an isobath of narrow bottom stripe can be represented periodically, or these data can be represented on a monitor.

It should be noted that in addition to the multibeam echosounder, other devices that measure depths simultaneously in several points of the ocean bottom have been developed, but all of them are based on the reflection of sound signals from the bottom.

If there are a lot of measurement data (more precisely this means that the average amount of measurement data

per surface area unit is relatively big, and the measurement points themselves are located uniformly on the surface investigated), then computer methods of isobath construction are used. In this case, two stages of the work are executed: first using the measurement data obtained in arbitrary points of the surface, the values of the depth in knots of a regular grid are calculated (sometimes this stage is known as digital surface model construction), and then using these grid values, coordinates of different isobaths are determined (grid values are used also for other forms of bathymetric mapping representations, 3-D views, for example). There are many algorithms of digital model creation, such as the least mean square method, and the so-called Kriging method, as well as algorithms of constructing an isobath of its own using depth grid values. To construct a precise map of the region it is necessary to perform echosounding surveying on it in such a manner that map stripes, obtained in different vessel tracks, would be as close to each other as possible, or even overlap. After performing such surveying, all data are joined together, and the map of the entire region is constructed.

It should be noted that currently, only small part of Earth's ocean bottom (several percent) is covered by such precise measurements. In some places, little data is available in a study area, obtained by one beam echosounder, or there is no data at all. In these cases, scientists try to use results of other geophysical measurements, first of all gravimetric measurements, to determine ocean depth. For example, methods of determination of ocean bottom topography using satellite altimetry or marine gravimetry data are useful. Even with using otherwise accurate satellite technology, indirect geophysical methods for determining the ocean bottom depth can always contain a mistake. The Earth's surface is a very complex formation, so the precise value of the ocean depth at a given point should be determined if necessary only by direct measurement.

In the case where depth measurement data are small in numbers for a given region, indirect methods are used in constructing bathymetric mapping, such as geomorphology analysis, for example. Scientists also take into account geological considerations and even human intuition, which can at times be useful.

Several international organizations are currently working on bathymetric mapping. The unclassified *General Bathymetric Chart of the Oceans* (GEBCO, in the scale 1:5000000), which may be considered a reference map, is one example. In this map, data of many regional bathymetric maps are collected, taking into account the different methods of their construction. There is also a digital version of this map (on CD), where files are represented in different formats, and in ASCII codes in particular, and where isobaths are represented in the so-called vector format.

Bathymetric mapping is finding increasing scientific and commercial use. For example, bathymetric maps are important in forging different underwater communications.

## ■ FURTHER READING:

### BOOKS:

Barnes, J. *Basic Geological Mapping*, 3rd ed. New York: John Wiley and Sons, 1995.

### PERIODICALS:

Perez, P. "SPOT Satellite Data Analysis for Bathymetric Mapping." *Image Processing*, vol. 3 (2000):464–467.

Opderbecke, J. "Depth Image Matching for Underwater Vehicle Navigation." *Image Processing*, vol. 2 (1999):624–629.

### SEE ALSO

*Mapping Technology*

## Baton Rounds.

SEE *Less Lethal Weapons Technology*.

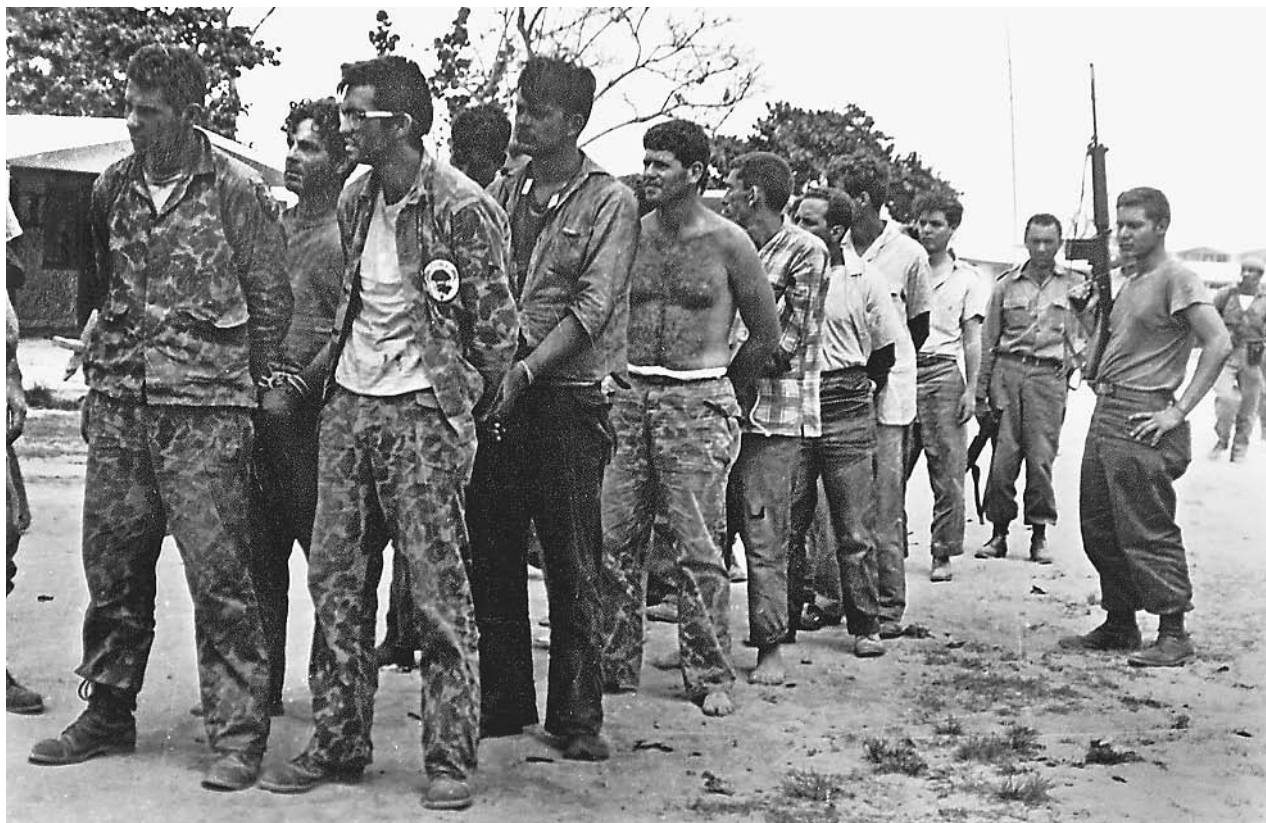
## Bay of Pigs

### ■ LARRY GILMAN

The Bay of Pigs (Bahía de Cochinos) is a small bay on the southern coast of Cuba that was invaded on April 17, 1961 by approximately 1,400 Cuban exiles organized and armed by the United States Central Intelligence Agency (CIA). The invasion was meant to appear to be an attempt by independent Cuban rebels to overthrow leftist Cuban leader Fidel Castro, but became obviously known as an American project, and confirmed when President John F. Kennedy immediately admitted responsibility when the invasion failed. The Bay of Pigs, as the whole episode came to be known, was a major embarrassment for the United States, which was caught deceiving the United Nations and trying to overthrow by force a government which the U.S. itself had officially recognized and which was not attacking the U.S. One hundred and fourteen invaders and 157 Cuban soldiers were killed and 1,189 invaders were taken prisoner.

Fidel Castro became the leader of Cuba's government when his revolutionary forces overthrew the Batista regime in January, 1959. At first, Washington was not hostile to Castro. President Dwight D. Eisenhower recognized his government a few days after Batista's downfall, and Castro even traveled to Washington to meet with Vice President Richard Nixon (later President Nixon). Nixon decided that Castro could not be relied upon to pursue U.S. interests and began to agitate privately for his removal.

In October, 1959, Eisenhower approved a secret program to depose Castro proposed by the CIA and the State Department. Eisenhower told his advisors that "our hand should not show in anything that is done"—in other words, that the operation should be carried out in such a way that



Cuban counter-revolutionaries, members of Assault Brigade 2506, after their capture at the Bay of Pigs, Cuba, in April 1961. ©AFP/CORBIS.

U.S. responsibility could be plausibly denied. To this end, the CIA gathered, funded, armed, and trained an anti-Castro rebel organization in Florida, the Panama Canal Zone, and Guatemala. The CIA began military training of 300 Cuban expatriates in March of 1960, and in May began broadcasting anti-Castro propaganda over the whole Caribbean from a station on a small, disputed territory named Swan Island. The programs were taped in Miami under CIA control, but claimed to be the voice of an authentic Cuban rebel movement without U.S. ties. In September, addressing the General Assembly of the United Nations, Castro accurately accused the U.S. of operating Radio Swan; the U.S. denied the charge.

In July, 1960, the Cuban fighters of "Brigade 2506"—named for the number of a brigade member killed in an accident—were transferred to a training camp in Guatemala built and run by the CIA.

On November 4, 1960, John Kennedy was elected president. Once in office, Kennedy gave his approval for the training of Brigade 2506 to continue. Like Eisenhower before him, however, Kennedy was adamant that U.S. armed forces should not take part in any effort to overthrow Castro. Not only was the whole operation illegal, any hint of U.S. manipulation would alienate potential supporters of the invasion inside Cuba. U.S. planners hoped that when news of the invasion reached the Cuban populace, an anti-Castro rebellion would arise and cast

him out. At the very least, planners believed, the invaders could fight their way overland to the Escambray Mountains, about 100 miles west of the landing zone, and join rebel forces already fighting there.

On April 15, 1961, the first part of the invasion plan was carried out. Eight B-29 bombers supplied by the CIA bombed Cuban military aircraft on the ground at several locations. Later, a B-26 bearing Cuban markings and marked with bullet-holes landed at Miami International Airport. The pilots claimed to be defecting Cuban pilots, the goal being to make the raids on Cuba earlier that morning look like an internal action by defecting Cuban pilots. However, reporters on the scene noted that the plane's machine guns had not been fired and that the plane was not of the type actually used by Cuba. Castro, hearing the reports, commented that even Hollywood would not have tried to film such a feeble story. The goal of the bombings themselves was to destroy the Cuban government's small air force at one stroke, eliminating any call for U.S. air support of Brigade 2506 at the landing site. The raid was not completely successful, however.

Two days later, on April 17, a landing was made at Playa Girón (Girón Beach) in the Bay of Pigs. A small beachhead was quickly achieved by Brigade 2506, but one of their freighter vessels, containing food, fuel, medical equipment, and a ten days' supply of ammunition, was quickly sunk. Combat was heavy around the beachhead as

Cuban government forces responded to the attack. The remnants of the Cuban Air Force bombed and strafed the invading forces, as Brigade 2506 had not been supplied with fighter aircraft and President Kennedy categorically refused to allow U.S. fighters to go into combat.

The military situation deteriorated steadily (from the invaders' point of view) over the next 48 hours. On April 18, while the fighting was at its peak, Adlai Stevenson denied to the United Nations, in response to Cuban accusations, that the U.S. was attacking Cuba. Eventually, Kennedy was persuaded to authorize unmarked U.S. fighter jets from the aircraft carrier *Essex* to provide escort cover for the invasion's B-26 bombers, most of which were now being flown by CIA agents in support of the ground invasion (two-thirds of the Brigade pilots were refusing to fly). The jets from the *Essex* missed their rendezvous with the B-26s by an hour due to a misunderstanding about time zones; in the subsequent, unescorted bombing raid over Cuba, two B-26s were shot down and four Americans were killed. The fighting ended on April 20, 1961, with the defeat of Brigade 2506.

The project, most analysts would later conclude, had been hopeless from the beginning. Fidel Castro enjoyed wide support in Cuba and had just consolidated a military victory against the Batista regime; a few thousand lightly-armed invaders could not possibly have taken the island. Furthermore, the idea that the U.S. could keep its role secret had become ridiculous long before the invasion was attempted. The *New York Times* had run a story on March 17, 1961, predicting a U.S. invasion of Cuba in the coming weeks, and another story on April 7, entitled "Anti-Castro Units Trained to Fight at Florida Bases," which noted that invasion plans were in their final stages. Although the *Times* had watered down the latter story considerably at President Kennedy's personal request, when Kennedy saw the paper he exclaimed that Castro didn't need spies; all he had to do was read the news. But Castro, and others, did have spies, and the Soviet Union was fairly well-informed of U.S. invasion plans ahead of time.

The costs of the Bay of Pigs were high, and not only in lives lost. In the wake of the invasion, Castro consolidated his regime, supported by public outrage in Cuba over the U.S.-plotted invasion, and concluded a mutual-defense agreement with the Soviet Union. The Soviet Union exploited this relationship to get Cuban permission to place ballistic-missile launch sites on Cuban soil. These launch sites, detected by U.S. aerial photography, were the immediate cause of the Cuban Missile Crisis of 1962, generally agreed to have been the closest approach to all-out nuclear war that the world has yet encountered.

#### ■ FURTHER READING:

##### BOOKS:

Blight, James and Peter Kornbluh. *Politics of Illusion: The Bay of Pigs Invasion Reexamined*. Boulder, CO: Lynne Rienner Publishers, 1998.

Kornbluh, Peter. *Bay of Pigs Declassified: The Secret CIA Report on the Invasion of Cuba*. New York: The New Press, 1998.

##### SEE ALSO

*Cuban Missile Crisis*  
*Kennedy Administration (1961–1963), United States National Security Policy*

## Belgium, Intelligence and Security Agencies

Officially upholding a declared policy of neutrality, Belgium maintains a small number of defense, intelligence, and military forces. Belgium has three national languages, French, German, and Dutch, all of which are equally recognized for official government use. The nation's central geographic location, varied linguistic structure, and policy of neutrality have aided the growth of Brussels as an international city and financial center. The Belgian capital also serves as the capital of the European Union (EU). With this added international responsibility, the Belgian government restructured many of its intelligence and law enforcement agencies in the early 1990s. National agencies work closely with other EU member nations to provide security in the international capital.

Belgium maintains both military and civilian intelligence forces. The nation's armed forces have various small, strategic intelligence units, but the Permanent Committee for the Control of Intelligence Services coordinates wide-scale military intelligence operations. The central committee, a branch of the Ministry of Defense and the General Intelligence Service, governs various operational divisions responsible for intelligence and security. The committee also coordinates joint operations with military and civilian security services.

The Intelligence Division of the Ministry of Defense manages external intelligence operations. Charged with protecting Belgian national interests at home and abroad, the Intelligence Division cooperates with military intelligence to gather, process, analyze, and act upon information. Mainly focusing on information from and about foreign states, the Intelligence Division maintains a small operational division.

A second operational division in the Belgian intelligence community is the Security Division. Charged with the protection of military security and classified information regarding foreign agreements, the Security Division conducts surveillance of military property and operations. The Security Division also screens government and military officials for various security clearances, granting access to classified materials.

The Security Intelligence Division, the third operational division of Belgian intelligence under the Ministry of Defense, is the nation's primary counterintelligence and counterespionage force. The division protects military operations and Belgian interests by seeking information relating to terrorism, sabotage, and espionage. The Security Intelligence Division sometimes works with other Belgian and European Union intelligence agencies to ensure the safety of EU officials, diplomats, and attaches in the capital and abroad.

Belgium maintains a smaller civilian intelligence force. The Ministry of Justice controls the Federal Intelligence and Security Agency, whose prime mission is the maintenance of state security. In the 1990s, the agency overhauled government information and computer systems to ensure the security of classified material. The agency works closely with law enforcement, and focuses on internal intelligence information.

As terrorist threats against European targets have increased, the Belgian intelligence community has increased efforts to protect EU government interests in Brussels. Belgium also pledged its support to an international anti-terrorism coalition.

#### SEE ALSO

*Counter-Intelligence*  
*European Union*

## Belly Buster Hand Drill

The "belly buster" hand-crank drill served as an aid to audio surveillance efforts by the United States Central Intelligence Agency (CIA) during the 1950s and 1960s. Designed to drill holes into masonry, the device made it possible to implant audio devices for covert listening.

The field of audio surveillance was already some 90 years old, as evidenced by the enacting of the first state statutes forbidding the interception of telegraphic messages in 1862, when the belly buster hand drill made its debut. It has long since become a museum piece, replaced by more sophisticated electronic drills, yet its genius lay in its sheer simplicity.

The drill, on display in the CIA Museum at agency headquarters in McLean, Virginia, was actually part of a kit that included several bits and accessories, including wire and microphones. The flat, compact kit made it easy to conceal, and once the operator arrived at the site of the intended audio surveillance, it could be assembled rapidly.

Having selected the area of wall to be drilled, the agent held the base of the drill against his stomach, and cranked the handle manually. The difficulty of this operation, and the exertion it placed on the operator's stomach,

earned the drill the nickname by which it is known to posterity.

#### ■ FURTHER READING:

##### BOOKS:

O'Toole, G. J. A. *Honorable Treachery: A History of U.S. Intelligence, Espionage, and Covert Action from the American Revolution to the CIA*. New York: Atlantic Monthly Press, 1991.

Owen, David. *Hidden Secrets*. Buffalo, NY: Firefly Books, 2002.

Pollock, David A. *Methods of Electronic Audio Surveillance*. Springfield, IL: Thomas, 1973.

##### ELECTRONIC:

"'Belly Buster' Hand-Crank Audio Drill." Central Intelligence Agency. <<http://www.cia.gov/cia/information/artifacts/belly.htm>> (January 6, 2003).

## Berlin Airlift

■ ADRIENNE WILMOTH LERNER

Following World War II, Germany was partitioned into various zones under the control of Allied nations. Berlin, the nation's key city, was also divided into different occupation areas, despite its location deep into the Soviet sector. Tensions escalated between the Western Allies and the Soviet Union, prompting the Soviets to attempt to take over control of all of Berlin. When France, Britain, and the United States agreed to introduce a new currency into their sectors in West Germany and Berlin, the Soviets declared the new currency void in the eastern partition under their control. Days later, the Soviet government closed supply lines to West Berlin. The United States Air Force and the British Royal Air Force organized a massive effort to deliver needed food, coal, and medical supplies into Berlin to thwart the Soviet blockade. The round-the-clock operation, which became known as the Berlin Airlift, sustained the residents of West Berlin for over a year, and secured the freedom of West Berlin from Soviet control.

**The Soviet blockade.** Berlin lay more than 100 miles (160 kilometers) inside of the Soviet-controlled eastern sector. The western sectors of the divided city relied on railroads and the Autobahn, the nation's main roadway, for the free transport of goods and supplies into the city. Berlin's eastern sector was controlled by a Soviet installed communist dictatorship, and was already experiencing shortages of essential goods and a fragile economy. West Berlin flourished under the control of the Western Allies,



Berlin children cheer as United States armed forces airlift supplies to West Berlin in 1948 after the Communists sealed off the borders.

©BETTMANN/CORBIS.

who intended to establish a democratic government and market economy, aid Germany in overcoming the legacy of the Nazis, and relinquish control of their sectors. In order to gain full control of Berlin, Soviet and East German forces acted on government decrees to occupy and shut-down essential transport services, effectively laying West Berlin under siege.

On June 15, 1948, the Soviets declared the Autobahn closed, and established roadblocks to prevent Berliners from fleeing the city. Within a week, all traffic between the various sectors of the city was halted. On Jun 21, river barge traffic was outlawed. Two days later, all railroads into and out of West Berlin were closed. Berliners were then at the mercy of the Soviet government to provide food and supplies. On June 24, 1948, the Soviets announced that they would not supply food to residents outside of the Soviet controlled sector. With all other means of transport cut-off, Britain and the United States, with the help of France, organized a massive airlift to feed and supply the sectors of West Berlin under their control.

**Military airlift operations.** Airlift operations began immediately. On June 26, two days after the Soviet announcement of the blockade, the United States Air Force airlifted the first cargo into Berlin. The American nicknamed the effort, "Operation Vittles," while British pilots dubbed the operation "Plain Fare." In July 1948, the operation was renamed the Combined Airlift Taskforce.

In the first months of the operation, the airlift gained international fame for delivering food and coal to blockaded Berliners. C-54 pilot, Lt. Gail Halverson added bundles of gum and candy to his payload for the crowds of children he noticed near the airfield. Halverson's "candy bombs" gained renown, and soon donations of candy and gum flooded his mailbox. In anticipation of winter, clothing donations were also collected from U.S. citizens and

businesses for transport to Berlin. Red Cross medical supplies were shipped in the airlift, and passengers were permitted to travel between West Germany and Berlin on a limited basis.

Airlift operations were conducted daily, often in inclement weather. Squadrons of American C-54s and British Dakotas, Yorks, Sunderland "Flying Boats," and Hastings aircraft delivered tons of goods per day to West Berlin. The sorties flew in tight patterns, landing sometimes as frequently as four planes a minute into one of three Berlin airfields. At the height of the airlift, as preparatory efforts for the winter of 1949 were underway, British forces drafted commercial airliners into service. The maximum effort launched by the Combined Airlift Task Force occurred on April 16, 1949. Known as the "Easter Parade," the airlift delivered 12,940 short tons of cargo, in 1,398 individual sorties, in one day.

Sustained airlift operations required a large-scale military effort not only in the air, but on the ground as well. Since Britain and France were still coping with post-war shortages at home, most supplies were shipped from the United States across the Atlantic in C-82 "Flying Boxcars." Cargo was shipped to American, British, and French bases in West Germany for final transport to Berlin. Once in Berlin, cargo from American C-54s required hand loading and unloading because the modified aircraft could not support pallet loads. Sacks of flour, coal, and other goods then were transported to locations established for distribution.

Major General William H. Tunner commanded the operation with the assistance of a deputy officer, RAF Air Commodore, J. F. Merer. Under their direction, the airlift employed increasingly complicated flying maneuvers and sophisticated technology to maximize the amount of cargo delivered to Berlin. The command team was primarily concerned with operational safety, since planes were required to fly at full tonnage, for long flights, in tight flying and landing patterns. Constant revision of safety standards and operational procedures, the instillation of sophisticated ground radar, as well as increased pilot training, aided the success of the Berlin Airlift while minimizing casualties and accidents.

The Soviets made no effort to stop the airlift. Soviet intelligence reported regularly on airlift operations and the condition and moral of West Berlin residents, but Soviet officials believed that the international coalition would fail or eventually abandon their efforts. Also, they were afraid that military intervention to prevent the airlift might result in another war.

On May 12, 1949, the Soviets finally lifted the blockade on Berlin. Train and auto transport was resumed into the city, but were limited at first. West Berliners regained their freedom to travel to West Germany several months later. Airlift operations continued through September of 1949 until supplies regularly reached Berlin via train and truck. In all, the Berlin Airlift delivered 2.4 million tons of

food and supplies in nearly 300,000 missions. Seventy-nine people lost their lives in the international effort to end the Soviet blockade.

**Legacy of the Berlin airlift.** The Berlin Airlift was the first large-scale, modern humanitarian effort that utilized airplanes as a primary means of delivery. The political effort was the first international humanitarian coalition that used military vehicles, installations, resources, personnel, and aircraft, instead of relying on civilian aid organizations. Setting the precedent for future aid operations, the success of the Berlin Airlift added a new role to peace and wartime military forces. Modern wartime humanitarian relief operations, as well as nation building policies were forged after World War II.

After the success of airlift operations and the formal end of the Soviet blockade, there was no easing of political tensions between the Soviet Union and the other Allies. The Western Allies united their occupation zones and created a self-sufficient, democratic government in West Germany. The Soviet Union established a communist satellite state. East Germany became the most tightly controlled Soviet satellite nation, aiding Soviet espionage and intelligence operations throughout the Cold War. Berlin remained partitioned between East and West. Soviet and East German troops used increasing force to control the border between East and West Berlin, cutting off the East from Western visitors and influences.

The Berlin Wall was constructed in the early 1960s to permanently partition the city. The wall became a Cold War symbol of the division between East and West, democratic and communist. In 1989, the failing East German government passed a law limitedly opening the border between East and West Berlin. When East German citizens heard of the law, they stormed the Berlin Wall and its guarded gates, demanding their immediate, and full, opening. East Germany, and the Berlin Wall, fell within months. The subsequent reunification of Germany brought the full end to the crisis which began with the Berlin Airlift forty years prior.

#### ■ FURTHER READING :

##### BOOKS:

Haydock, Michael D. *City under Siege: The Berlin Blockade and Airlift, 1948–1949*. Washington, D.C.: Brassey's, 2000.

Miller, Roger G. *To Save a City: The Berlin Airlift, 1948–1949*. Seattle, WA: University Press of the Pacific, 2002.

##### SEE ALSO

*Cold War (1945–1950), The Start of the Atomic Age*

*Cold War (1950–1972)*

*Cold War (1972–1989): The Collapse of the Soviet Union*

*Germany, Intelligence and Security*

STASI

*United Kingdom, Intelligence and Security*  
*United States, Intelligence and Security*  
*World War II*

## Berlin Tunnel

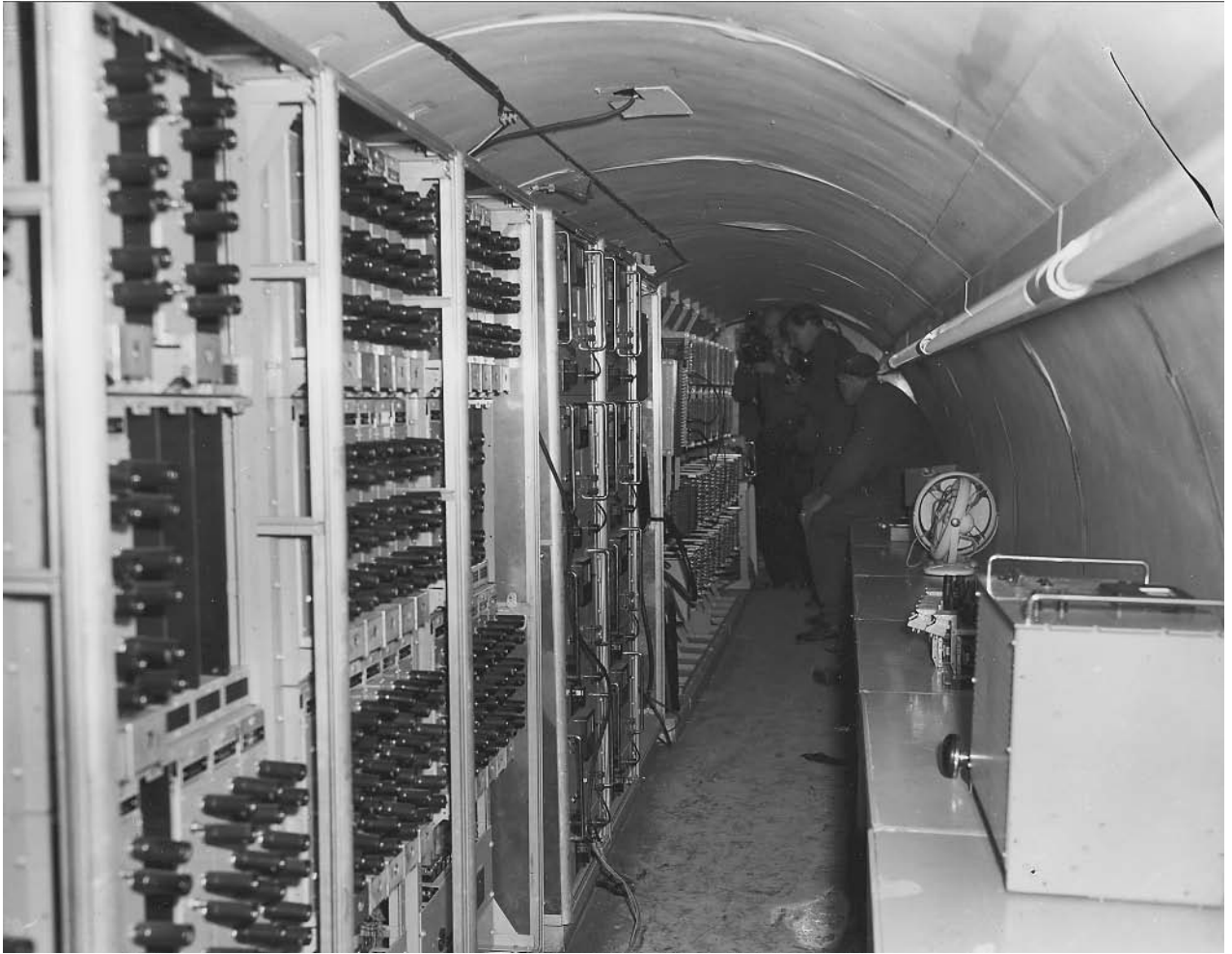
■ CARYN E. NEUMANN

The Berlin Tunnel involved an attempt by American and British intelligence to adjust to the late 1940s Soviet shift from wireless transmissions to landlines by tapping Soviet and East German communication cables via a tunnel dug below the communist sector of the German city. The tunnel, which lasted from March 1955 until its discovery by Soviet troops in April 1956, provided difficult-to-obtain military intelligence, as well as information about scientific and political developments behind the Iron Curtain.

The brainchild of the CIA, the Berlin Tunnel aimed to collect Soviet intelligence passed along an underground hub of telecommunications cables adjacent to the U.S. sector of the divided city. While Operation Gold had been conceived in 1951, detailed plans were not in place until August 1953 and the concept did not receive CIA approval until January 1954. The delays centered on the difficulty of discovering exactly which cables were used for Soviet communications and where these cables were located. While the CIA relied upon a number of East German sources to get information, a contact in the long-distance department of an East Berlin post office proved especially useful by providing books that identified cable users. Another contact in the East German Ministry of Post and Telecommunications provided detailed official maps of Soviet cable lines. Tunnel construction then began early in 1954.

The CIA, using the U.S. Army as a front, designed a warehouse that led to a subterranean passageway about 1800 feet long (900 feet into Soviet territory) and 16.5 feet deep. A West Berlin contractor built the warehouse under the misconception that the unusually deep basement and ramps to accommodate forklifts were part of a new and improved quartermaster warehouse design. A detachment of U.S. Army engineers dug the tunnel, but the British army drove the vertical shaft from the end of the tunnel to the target cables and British telecommunications experts made the actual tap. In order to disguise evidence of digging, the army installed washers and dryers on site to clean the fatigues of the construction workers. As a defense against possible Soviet attackers, a heavy torch-proof steel door separated the preamplification chamber, where the signals were isolated for recording, and the vertical shaft of the tap chamber. A microphone in the tap chamber permitted security personnel to monitor any





Soviet authorities find amplifiers and other equipment used to tap Russian telephone lines inside the long tunnel in Berlin, Germany, during the Cold War in 1956. Russian officials discovered the tunnel, and charged that it was dug by the American authorities from their Berlin sector across the border. AP/WIDE WORLD PHOTOS.

activity in the area. Sandbags along the tunnel walls muffled sounds and served as shelves. Construction of the entire tunnel complex ended in March 1955 and the taps began in May.

The KGB soon became aware of Operation Gold through George Blake, a Dutch-born British double agent for the Soviets who entered MI-6 in 1953. Blake, employed in a technical division, gave information about the tunnel to the KGB when the project was still in the planning stages. In order to attack the tunnel, the Soviets would have to compromise Blake and they found it preferable to sacrifice some information rather than their valuable agent. The KGB did not inform anyone in Germany, including the East Germans or the Soviet users of the cable lines, about the taps. When Blake received a transfer in 1955, the Soviets were free to “discover” the tunnel.

Soviet and American accounts of the tunnel discovery do not match, with the Soviets creating a fanciful and widely-circulated account of Soviet technicians surprising

Americans as they sipped coffee in the tunnel. In reality, with Blake safely out of the way, Soviet Premier Nikita Khrushchev planned to use the tunnel to score propaganda points but he did not wish to embarrass the British government on the eve of his visit to the island nation. He planned to emphasize the American role in the tunnel while downplaying British involvement. Accordingly, Soviet troops began to dig on the night of April 21, 1956. American personnel, using night vision equipment, detected 40 to 50 Soviet soldiers digging at three to five foot intervals. Given ample warning, the Americans retreated behind the steel door. The Soviets, unable to open the door, dug through an adjacent wall to get into the preamplification chamber. Once inside, they cut the tap cables and the microphone went dead.

Although it came to an embarrassing end, the Berlin Tunnel counts as a successful intelligence operation. The American and British governments used 50,000 reels of tape to capture 443,00 fully transcribed conversations

(368,000 Soviet and 75,000 East German), which in turn led to 1,750 intelligence reports. Besides revealing the latest developments in Soviet atomic research, the tapes indicated disagreements between the Soviets and the East Germans over the status of West Berlin. Despite Soviet claims to the contrary, the tunnel provided much more than carefully planned misinformation.

## ■ FURTHER READING:

### BOOKS:

Miller, Nathan. *Spying for America: The Hidden History of U.S. Intelligence*. New York: Paragon House, 1989.

Murphy, David E., Sergei A. Kondrashev, and George Bailey. *Battleground Berlin: CIA vs. KGB in the Cold War*. New Haven: Yale University Press, 1997.

### SEE ALSO

*CIA (United States Central Intelligence Agency) Cold War (1950–1972)*

*KGB (Komitet Gosudarstvennoi Bezopasnosti, USSR Committee of State Security)*

*MI6 (British Secret Intelligence Service)*

---

## Berlin Wall

---

### ■ DAVID TULLOCH

In the early hours of August 13, 1961, the border crossings between the eastern Soviet Occupied Zone of Berlin and the western American, British and French controlled sectors began to be sealed. At first barbed wire was used to separate East from West Berlin, but over time this was replaced by concrete slabs and a deadly no man's land that became known as the Berlin Wall. The Wall split a city, a people, and the world, tearing apart families and friends for decades, and becoming a powerful symbol of the Cold War, representing the deepening divide between East and West, physically, politically, and philosophically.

## After the Second World War

Well before the D-Day invasion of mainland Europe, the three main Allied powers, Britain, the United States, and the Soviet Union, held high-level discussions to determine how to administer Germany after it had been defeated. Eventually it was decided that Germany would be split into four administrative zones, one each for the Soviets, the American, the British, and the French. Berlin, as the German capital, was also to be divided into four administrative zones. However, Berlin was located deep within the zone allocated to the Soviets, 180 kilometres (110 miles) from the western zones, and this geographical fact was to haunt post-war Germany for many decades.

Immediately after the war, the major concerns of the administrative powers were feeding the populace, and coping with the severe winter of 1947. The major political discussions were disagreements over the amount of reparations Germany could pay while still leaving it with sufficient resources for recovery. However, the “Berlin Problem,” as it came to be known, was also beginning to surface.

Post-war military rule by the four powers was intended to be a short term measure, as it was assumed a suitable German civilian government would be quickly formed, and the Allies would then sign a peace treaty with this new authority and withdraw their troops. As a result, there was little or no long-term planning in regards to the peculiar problems of Berlin. Access routes from the western zones were only tenuously agreed upon with the Soviets. The notion that both Germany and Berlin would remain divided for an extended period was just not considered. When relations between the Soviet Union and the Western powers began to deteriorate, all sides found themselves with a geographical problem that caused political problems.

**The Cold War heats up.** The first major crisis between East and West regarding post-war Germany began on June 24, 1948, when Western land access to Berlin was blocked by the Soviets. Berlin relied on shipments of almost every good its population used, from food and medicine to coal for heating and power generation. At first it appeared that the Western powers would be forced to either abandon their sectors of Berlin, or open a land passage to Berlin through military confrontation, risking a possible Third World War. Unexpectedly, however, it proved possible to supply Berlin with the bare essentials (and no more) through a massive airlift operation. The New York Treaty of May 4, 1949 effectively ended the Berlin blockade, and the Western counter-blockade, and supplies quickly returned to normal levels.

The blockade effectively ended the charade of four power cooperation in the administration of Germany and Berlin, with the Soviet sector eventually becoming the German Democratic Republic (GDR) and the Western sectors eventually becoming the Federal Republic of Germany (FRG). In both cases, however, Berlin was considered the capital city of these new countries, but a Berlin divided between the Soviets and the West. The events of the blockade were also a fundamental impetus behind the formation of the North Atlantic Treaty Organisation (NATO), and its Eastern counterpart, the Warsaw Pact, further defining the divisions of the Cold War.

**Refugees.** The 1950s saw both sides of Berlin turned into political and social showrooms for the competing doctrines. West Berlin developed into a capitalist Mecca, while the East of the city transformed into a model socialist city. While the border between the two areas was sealed in 1952, this did not stop half a million people



The Brandenburg Gate was sealed off by the Soviets in the Soviet-occupied sector of East Berlin in 1961. Located at the center of the German capital, the gate stood at the divide between East and West Berlin until the wall was torn down by German authorities and citizens in 1989. AP/WIDE WORLD PHOTOS.

crossing the borders each day. Many East Berliners worked in the West, where they could make more money and so enjoy a higher standard of living than those working in the East, a situation that led to resentment from some. Berliners from the West enjoyed the extra spending power their currency offered in the East, crossing the border for less expensive haircuts, clothes, and other goods and services. Relatives living on opposite sides of the city could visit each other, students crossed to attend schools and universities, and many people crossed the border to attend concerts and sporting fixtures. There were some measures introduced to make crossing the border difficult and frustrating, such as police controls on many crossing points, and the barricading of some streets, but over 80 access points still remained open, and the underground railway (S-bahn) still crossed regularly.

However, there were a large number of people crossing from the East who simply did not return. Towards the end of the Second World War there had been a flood of refugees fleeing from the East to the West ahead of the

advancing Soviet army. While the tide slowed after the end of the war, there remained a steady stream of Germans who left the East of the country and resettled in the West. It is estimated that more than two and a half million East Germans fled into the West between 1946 and 1961, yet the entire population of East Germany was only 17 million. The East German authorities attempted to restrict their citizens crossing by introducing passes and making "fleeing to the Republic" a crime with potential jail sentence of up to four years.

There were many factors driving the refugees. Some were as basic as seeking a better job, more food, or more material goods. The numbers of refugees spiked upwards during times of hardship in the East, when food and other essential resources were scarce. The social and political changes that had taken place in the Soviet zone, such as the educational reforms and the removal of many judges from their positions, resulted in many educated and wealthy persons moving to the West. The refugee problem grew and became an embarrassment for both sides. The East

viewed those leaving as traitors and the West could not cope with the scale of the human tide. In the first seven months of 1961, over 150,000 East Germans left for the West. Walter Ulbricht (1893–1973), the leader of East Germany, repeatedly requested that he be able to take radical measures to stop the problem, but he was denied, at least for the time being.

**The Berlin crisis.** Aside from the refugee problem, there were political troubles that threatened not only the peace and stability of Berlin and Germany, but also the world. In 1958, the Soviet Leader, Nikita Khrushchev (1894–1971) demanded that several thorny post-war issues be resolved within a six-month period. The Soviets wanted negotiations on European security, an end to the four-power occupation of Germany, a final peace treaty signed with a reconstituted Germany, and the creation of a nuclear-free Germany to act as a buffer zone between the two superpowers.

The Soviets threatened that if their demands were not met then they would sign a separate peace treaty with East Germany, officially splitting Germany in two (even if in practice it already was so.) Summit talks were held in Geneva (May–August 1959), Paris (May 1960), and with the newly elected President John F. Kennedy (1917–1963) in Vienna (June 1961), but no agreements were forthcoming.

On the night of August 12, 1961, on the Eastern side of Berlin, large numbers of army units, militiamen, and People's Police (Vopos) began to assemble near the border. Beginning shortly after one in the morning the troops were posted along the border, and the wire and posts were deployed to seal East from West Berlin. Traffic was prevented from crossing, including the underground railway trains. When Berliners awoke on the morning of August 13 their city had been split in two.

The closure of the border between the two halves of Berlin came as a surprise to Western intelligence agencies. After the fact, a number of reports and individuals surfaced claiming to have foreseen the events of August 13, but at the time there was no credible source that was believed by the West. Some historians have suggested there was an overload of information at the time, with too many spies and informers supplying information. Sorting through the sheer volume of reports was one problem, as well as sorting the useful signals from the noise of half-rumor and disinformation. Reports from civilians who noticed that something “big” was occurring before the border was sealed were dismissed, as they were considered less reliable than the professional spies and informers. Credit must also be given to the secret planning and execution of Ulbricht, Erich Honecker (1912–1994), and their forces, who managed to stockpile 40 kilometres of barbed wire and thousands of posts without arousing suspicion. Even as the border was being sealed, many people on both sides had no idea what the ultimate purpose was, including those laying out the barbed wire.

The initial Western lack of response was baffling to many, who expected a more aggressive approach from the Western military in Berlin. The Kennedy administration appeared to accept that the Soviets had a natural right to protect their borders, and the other Western leaders followed his lead. Despite the fact that the East German actions violated the agreements the Four Powers had made after the Second World War, the United States only protested in a feeble manner. While Kennedy has been criticized heavily by biographers and historians for doing nothing, in effect, the lack of an active Western response stabilized the situation. While tension remained high for the next two years, the walling of the Berlin border did not threaten to boil over into armed conflict in the same manner as the Berlin Blockade had done.

If there had been too much intelligence information before the Wall, after the border was sealed there was the opposite problem. Before the Wall, spies crossed as easily as anyone else did. The massive tide of refugees that moved to the West Berlin before the sealing of Berlin caused many intelligence problems, as it was simply not possible to effectively screen all potential communist agents when the numbers crossing were high. After the wall, it became much harder to send spies across the border, simply because there was no longer any civilian traffic. Potential spies were now much easier to spot, and security forces on both sides could now shadow all suspected persons in official parties who crossed the divide.

Over the years, the East Germans modified and added to the initial barbed wire fence between the two Berlins. As soon as it became obvious that the West was not challenging the erection of the barricades, the first concrete sections were moved into place. Within the first few months, the Wall began to take on a more permanent shape, consisting of concrete sections and square blocks. Weak points were quickly identified and sealed. In mid-1962, modifications were made to strengthen the Wall, and in 1965, a third generation of Wall building began, using concrete slabs between steel girders and concrete posts. The last major reconstruction of the Wall began in 1975, when interlocking concrete segments were used.

The border fencing off West Berlin from East Germany was 155 km. (96 mi.) in length. The actual concrete structure that became infamous was only 107 km. (66.5 mi.) in length, the remainder of the border was sealed off by wire and fences. More than 300 watch towers were built along the border, as well as 105 km. (65 mi.) of anti-vehicle ditches, more than 20 concrete bunkers, and all patrolled by several hundred dogs and more than ten thousand guards.

While the Wall was a formidable barrier that did not stop many East Germans from trying to cross it. In the first few days and weeks of its construction there were many gaps in the border. Escapees jumped, burrowed, climbed, and swam their way through weak points in the fence. Some East German residents lived in apartments that had windows and doors that opened into the West. Some fled to West Berlin simply by walking through their front doors,

and when they were sealed, by climbing out the windows. Over time the holes and weak points in the Wall were found and blocked. Those attempting to escape in later years faced many more hazards, and while some were successful, many were wounded or killed in the attempt.

**The fall of the Wall.** The collapse of the Wall was an even greater surprise than its construction, catching the East German politicians and border guards unaware. In 1989, there had been growing unrest in the GDR, with a number of mass demonstrations in East Berlin. A new refugee crisis was also causing problems for the East German authorities. The August, 1989, the opening of the Hungarian border with Austria provided a new gateway to the West. In just three days of September, 1989, over 13,000 East Germans fled to the West via Hungary. The East German authorities rushed through a number of stop-gap measures in an attempt to stem the flow of refugees, including the forced resignation of Honecker on October 18, and giving amnesty to those who had attempted to cross the border illegally. However, the unrest continued, and the refugees still fled.

Then on November 9, 1989, Politburo member Guenter Schabowski gave a television interview in which he announced that East Germans would be able to travel abroad. When a reporter asked when this would apply Schabowski seemed unsure, but then said "immediately." Within minutes, crowds gathered at the border demanding to cross, but the guards refused to let them pass without orders. The East German authorities had intended for the new travel conditions to apply the next day, but in order to avoid violent confrontations, the border was opened. Huge crowds crossed the border, and an impromptu celebration erupted in both sides of Berlin. The Wall had been breached, and would not be closed again.

#### ■ FURTHER READING:

##### BOOKS:

- Hilton, Christopher. *The Wall: The People's Story*. Stroud, Gloucestershire: Sutton Publishing, 2001.
- Read, Anthony and David Fisher. *Berlin: The Biography of a City*. London: Pimlico, 1994.
- Tusa, Ann. *The Last Division: A History of Berlin 1945–1989*. Reading, MA: Addison-Wesley Publishing, 1997.

##### ELECTRONIC:

- Berlin Wall Online. <<http://www.dailysoft.com/berlinwall/>> 2003.
- Deutsches Historisches Museum Berlin <<http://www.wall-berlin.org/>>.

##### SEE ALSO

- Berlin Airlift*  
*Berlin Tunnel*  
*Cold War (1950–1972)*  
*Cold War (1972–1989): The Collapse of the Soviet Union*

## Biochemical Assassination Weapons

■ JUDYTH SASSOON

Assassination is usually defined as politically inspired murder. The term is probably derived from the Arabic word for hemp (Hashish), which was apparently used by Hasan-ban-Sabah (c. 1034–1124) to induce motivation in his followers. These "hashishins" or assassins were assigned to carry out political and other murders, usually at the cost of their own lives. Thus, at the etymological level, there is already a connection between assassination and compounds derived from nature.

Biochemicals in the context of assassination involve mostly plant-derived drugs or toxins. They can be organic compounds such as alkaloids, diterpenes, cardiac and cynogenic glycosides, nitro-containing compounds, oxalates, resins, certain proteins and amino acids. A selection of these biochemicals were effectively used in assassination attempts throughout history.

The ancient civilizations of the Near East, Greece and Rome developed the use of poisons in political homicide to a high degree of efficiency. In classical Rome, mushroom poisons were expertly administered by Agrippina (A.D. 16– A.D. 59.), wife of Emperor Claudius and mother of Nero. She successfully disposed of several political rivals, including Marcus Silanus who was to succeed Claudius, and eventually Claudius himself. Agrippina probably employed the properties of the amanita species, which contain amanitin polypeptides that produce degenerative changes in the liver, kidney, and cardiac muscles. In ancient Egypt, Queen Cleopatra in her search for a suitable suicide compound became familiar with the properties of henbane (*Hyoscyamus niger*) and belladonna (*Atropa belladonna*), although she judged death by these plants to be rapid, but painful. Cleopatra was also disappointed with *Strychnos nux-vomita* (a tree whose seeds yield strychnine). Strychnine causes stimulation of the central nervous system, produces generalized convulsions, and distorted facial features at death. The latter did not suit Cleopatra, who eventually settled for the bite of an asp (Egyptian cobra), which produced a more serene and prompt death worthy of a queen.

Hemlock is another notorious biochemical used in political murders. The hemlock plant contains coniine, an alkaloid, and was used to execute the Greek philosopher Socrates (c.479 B.C.–399 B.C.). The drug causes progressive motor paralysis extending upwards from the extremities until death results from respiratory failure. Some of the deadliest political poisons were concocted by the alchemists of the Middle Ages. La Cantrella was a secret assassination weapon used by Cesare Borgia (1476–1507) and Lucrezia Borgia (1480–1519) to despatch their enemies. Even today, its exact composition is not known, but



Senator Frank Church, left, chairman of the Senate Select Intelligence Committee, displays a poison dart gun as co-chairman Senator John Tower watches during the panel's probe of the activities of the Central Intelligence Agency in 1975. AP/WIDE WORLD PHOTOS.

it was most probably a mixture of naturally derived copper, arsenic and crude phosphorus.

In later times, cyanide became more widely used as a homicidal poison. Today, cyanide is usually derived in large quantities from industry, but it has its source in biochemical processes involving cyanogenic glycosides. Amygdalin is one of the most widely distributed glycosides, yielding hydrocyanic acid (HCN) as a product of hydrolysis. It is present in the rosaceae plant family and found in the seeds of apples, cherries, peaches and plums. HCN inhibits the action of the enzyme cytochrome oxidase and prevents the uptake of oxygen by cells. As little as 0.06 g can cause death in humans. Consumption of a lethal dose of HCN is usually followed by collapse and death within seconds. As an assassination weapon, it was famously employed in the killing of the Russian monk Gregory Efimovich Rasputin (c.1872–1916). Legend has it that Rasputin's unnaturally strong constitution allowed him to ingest enough cyanide to kill six men, yet he continued to breathe and eventually received his *coup de grace* from a gun shot.

Ricin is a political poison of twentieth-century origin. It is found in the shell casing of castor beans and is easily produced, thus having the potential to be a large-scale murder weapon. Ricin came to public attention in 1978 when it was used in the assassination of Bulgarian dissenter Georgi Markov in the United Kingdom. Markov

worked as a broadcaster for the British Broadcasting Corporation, and relayed pro-Western material to his communist homeland. Markov died several days after being jabbed by an umbrella at a bridge in London. The poison-tipped umbrella injector was designed by the Soviet intelligence agency KGB, whose Bulgarian agent carried the umbrella and delivered the Ricin to the victim. An autopsy revealed that a platinum-iridium pellet the size of a pinhead had been implanted in Markov at the site of his injury. The pellet was cross-drilled with 0.016-inch holes to contain the Ricin. A short time earlier, a similar attempt had been made in Paris against another Bulgarian defector, Vladimir Kostov. This attempt proved unsuccessful because his heavy clothing prevented the steel ball from entering any farther than his subcutaneous tissue. Kostov read of his comrade's death and went for a medical examination during which the pellet was found and removed before any of the toxin could be absorbed. Ricin is an extremely toxic poison. It is estimated that Markov was killed by only a 425 mg. dose contained in the pellet. Ricin is deadly because it can be inhaled, ingested or swallowed and is quickly broken down in the body and is virtually undetectable. Markov's assassination was only detected because the pellet carrying the poison had not dissolved as expected. There is currently no antidote to Ricin although a vaccine has been developed that has been successfully tested in mice.

Apart from the poison pellet umbrella, the KGB is known to have designed several other imaginative devices to deliver biochemical poisons. One was a pen-sized assassination weapon that could deliver gas or liquid poisons. Another was a cigarette case, surrendered by KGB assassin Nikolai Khokhlov upon his defection to West Germany in 1954. The device could fire poison filled hollow-point bullets through the false cigarettes at the opening of the case. Khokhlov, who had been sent to assassinate anti-Soviet émigré Georgi Sergeyevich Okolovich, defected rather than carry out his mission.

In the 1950s and 1960s, a talented chemist and poisons expert worked for the United States Central Intelligence Agency (CIA). He was Sidney Gottlieb (1918–) and also operated under the name Joseph Scheider. In the 1960s, Gottlieb was involved in various chemical and biochemical projects, none of which was apparently successful. Gottlieb created devices that could deliver poisons by which the CIA could carry out assassinations of political leaders who were assumed to be a threat to U.S. national security. One of these leaders was Fidel Castro, whose liking for Havana cigars was considered to be a possible means of administering poison pellets. Gottlieb is thought to have inserted poison into Havana cigars that were sent to Castro, but which were somehow intercepted and never arrived. Gottlieb then tried to create a poisoned wetsuit, which Castro never wore. Another assassination attempt involving Gottlieb was planned by the CIA on General Abdul Karim Kassem of Iraq by planting a poisoned handkerchief in his suit pocket, but this plan also failed. Gottlieb adopted a slightly different tactic in the planned assassination of African leader Patrice Lumumba, the leftwing prime minister of the Congo (now Zaire). In September 1960, he constructed an assassination package that included a biological agent able to induce tularmia (rabbit fever), brucellosis (undulant fever), anthrax, smallpox, tuberculosis and Venezuelan equine encephalitis (sleeping sickness). This agent was mixed with toothpaste and placed in a tube that could be slipped into Lumumba's traveling kit. Gottlieb delivered this package to Lawrence Devlin, the CIA station chief, instructing him to kill Lumumba. However, the operation also did not achieve its aim, as Lumumba's enemies in the Congo murdered him first in January, 1961.

#### ■ FURTHER READING:

##### BOOKS:

Klaassen, C. D. *Toxicology: The Basic Science of Poisons*. McGraw-Hill Companies, 2001.

##### PERIODICALS:

Benomran, F. A., and J. D. Henry. "Homicide by strychnine poisoning." *Med Sci Law* 36 (1996): 271–3.

Dally, S. [Non-accidental criminal poisonings] *Rev Prat* 50 (2000): 407.

Knight, B. "Ricin—A Potent Homicidal Poison." *Br Med J*. 1 (1979): 350–1.

Vetter, J. "Plant Cyanogenic Glycosides." *Toxicol Chem* 38 (2000):11–36.

Zhan, J., and P. Zhou. "A Simplified Method to Evaluate the Acute Toxicity of Ricin and Ricinus Agglutinin." *Toxicology* 186 (2003): 119–23.

#### SEE ALSO

*Anthrax, Terrorist Use as a Biological Weapon*  
*Toxicology*  
*Toxins*

## Biocontainment Laboratories

■ BRIAN HOYLE

A biocontainment laboratory is a laboratory that has been designed to lessen or completely prevent the escape of microorganisms.

There are four levels of biocontainment laboratories. Each level must meet certain design criteria, and each is designed for research involving certain microbes. The four levels are designated as Biosafety Level (BSL) 1, 2, 3, and 4.

### Types of Biosafety Level Laboratories

The typical university research laboratory is a BSL-1 facility. Such a laboratory has few restrictions on who may enter, connects directly with the remainder of the building, and, other than the wearing of lab coats and observing normal lab hygienic practices, has few specialized safety features. For example, work is done on open-air bench tops without specialized equipment designed to contain the organisms (e.g., fume hood).

The safety features that are in place in a BSL-1 facility are routine. Examples include hand washing before and after work in the lab, decontamination of bench tops before and after use, restrictions on food and drink, and sterilization of all materials that have been in contact with microorganisms. The work space is constructed with sealed seams and a crevasse-free surface, to lessen the chances that microorganisms will pool in a hard-to-reach location and grow.

Personnel in a BSL-1 laboratory are trained in the techniques necessary to prevent contamination of the experiment or themselves. These techniques are not complex and undergraduate students can safely study in a microbiology teaching BSL-1 lab.

**BSL-2 Laboratory.** A BSL-2 laboratory is similar in design and operation to a BSL-1 lab. However, some additional



A research technician conducts experiments that include challenging insects with a virus mixed with blood at the U.S. Department of Agriculture Arthropod-Borne Animal Diseases Research Laboratory, a biocontainment laboratory that specializes in animal diseases that are transmitted by insects, including plague, West Nile, and tularemia. AP/WIDE WORLD PHOTOS.

safety features are in place to allow microorganisms that are potentially hazardous to health to be studied. For example, lab personnel are trained in the handling of specific disease-causing microorganisms, more care is taken when handling the microbes (i.e., wearing sterile gloves). Access to the BSL-2 lab is restricted and the doors remain closed when experiments are in progress.

Because of the presence of microorganisms that can pose an increased health threat, people who are known to have a less efficiently operating immune system are not allowed inside the laboratory. Even those with normal immune systems are tested regularly for evidence of infection, or can be vaccinated against the microbes they work with.

Procedures like blending and centrifugation create the opportunity for organisms to become airborne. Special protective clothing such as a facemask is worn, and biological safety cabinets are present. The location of the specialized equipment must be approved (i.e., a safety cabinet is not allowed to be by an open window or the door to a hallway).

There are no specific ventilation requirements for a BSL-2 laboratory. Air enters and exits the lab via the building's ventilation system. If windows are present, they can be opened.

**BSL-3 Laboratory.** This facility is designed for work with microorganisms that can easily become airborne and that

carry a great risk of infection. Often a BSL-3 laboratory is in a hospital or an infectious disease research facility.

One distinguishing characteristic of a BSL-3 laboratory, compared to BSL-1 and BSL-2 labs, is the requirement that work with the microorganisms be done within biological safety cabinets or other containment equipment, or by personnel wearing protective clothing (i.e., wrap-around gowns, scrub suits, coveralls, gloves that are changed frequently). Another characteristic is increased restrictions for access to the lab. For example, newer facilities must have double doors, which are sealed around their edges. The first door that connects to the outside of the lab must be fully closed before the door to the BSL-3 lab is opened.

Ventilation systems in the BSL-3 lab are independent from the rest of the building's ventilation system. The air from the laboratory is exhausted directly to the outside and not into the general building circulation. The exhaust air is also filtered to remove microorganisms. Also, ideally the airflow through the laboratory should be balanced (i.e., the air flow into the room is the same as the air flow out of the room) and should flow from areas that are not used for experimental work such as office space to areas containing the microorganisms.

The floors and walls of a BSL-3 laboratory are designed to be free of cracks, impermeable to fluids, and chemical resistant. While windows are permitted, they cannot be opened.

The satisfactory performance of all equipment and personnel in the lab is regularly monitored and recorded for inspection. The lab and the personnel are re-verified each year.

**BSL-4 Laboratory.** The BSL-4 facility is designed for work with microorganisms that pose a dire health threat. The most infectious microorganisms (i.e., Ebola virus, *Bacillus anthracis* (the cause of anthrax), the Marburg virus, and Hantavirus) can be handled only in a BSL-4 laboratory. A newly discovered microorganism that is genetically related to a known extreme pathogen will also be handled in a BSL-4 lab until, when, and if it is demonstrated that the organism does not pose a threat to health or life.

Two hallmarks of the microorganisms that can be handled only in a BSL-4 laboratory is their ability to be easily transmitted from and to people via the air, and from person to person (they are highly infectious). The design of a BSL-4 laboratory prevents the release of these microorganisms into the environment and protects the researchers from infection.

An example of a BSL-4 laboratory is the one that is present in the United States Army Research Institute of Infectious Diseases, in Fort Detrick, Maryland. At 10,000 square feet, the USAMRIID BSL-4 facility is the largest highest-level biocontainment laboratory in the United States. As of 2002, three other BSL-4 labs exist in North



America. The others are at the Centers for Disease Control and Prevention in Atlanta, Georgia, San Antonio, Texas, and Winnipeg, Manitoba, Canada.

A fourth BSL-4 laboratory is planned for the National Institute of Allergy and Infectious Disease's Rocky Mountain Lab in Hamilton, Montana.

The personnel who work in a BSL-4 laboratory have been highly trained and certified. They are experts in microbiological techniques and in the containment of infections. Only these lab personnel are allowed into the laboratory.

Entry to the Level 4 area requires passage through several checkpoints and the keying in of a security code that is issued only after the person has been successfully vaccinated against the microorganism under study.

All work in the level 4 lab is done in a pressurized and ventilated suit. Air for breathing is passed into the suit through a hose and is filtered so as to be free of microorganisms.

Standard operating procedures are in place for every technique and operation in a BSL-4 laboratory (i.e., changing a filter on a reverse osmosis filtration device), and all work done in the laboratory is documented.

A BSL-4 laboratory is completely isolated from the rest of the rooms in the building. Ideally, the lab is located in a separate building. The laboratory is designed to be a secure facility with respect to the escape of microorganisms. Until now, security against sabotage or deliberate damage has not been a design feature. However, this is changing. The BSL-4 laboratory proposed for Hamilton, Montana, will be in a fenced and guarded space, and will be equipped with observation cameras, multi-levels of secured access, and complete illumination of the exterior of the lab at night.

#### ■ FURTHER READING:

##### BOOKS:

Richmond, Jonathan Y., and Robert W. McKinney (eds.) *Biosafety in Microbiological and Biomedical Laboratories, 4th edition*. Washington, D.C.: U.S. Government Printing Office, 1999.

##### ELECTRONIC:

National Institute of Allergy and Infectious Diseases. "An Integrated Research Facility at Rocky Mountain Laboratories: Questions and Answers." Office of Communications and Public Liason. November 5, 2002. <<http://www.niaid.nih.gov/dir/infobs14/bs14faq.htm>> (06 December 2002).

USAMRIID. "Welcome to USAMRIID." The U.S. Army Medical Research Institute of Infectious Diseases. Fort Detrick, MD. July 25, 2002. <<http://www.usamriid.army.mil/>> (25 November 2002).

##### SEE ALSO

*Biological Weapons, Genetic Identification*

#### *Bioterrorism*

*Microbiology: Applications to Espionage, Intelligence and Security Pathogens*

## Biodetectors

■ JUDYTH SASSOON

Biodetectors are analytical devices that combine the precision and selectivity of biological systems with the processing power of microelectronics. Biodetectors act as powerful analytical tools in medicine, environmental diagnostics, and food industries, as well as forensic analysis and counterterrorism. Biodetectors usually consist of a biological recognition system, typically enzymes or binding proteins immobilized on a surface acting as a physico-chemical transducer. One typical example of a biodetector is the immunosensor, which uses antibodies as the biorecognition system. In addition to enzymes and antibodies, the recognition systems can consist of nucleic acids, whole bacteria and single cell organisms and even tissues of higher organisms. Specific interactions between the target molecule or analyte and the complementary biorecognition layer produce a detectable physico-chemical change, which can then be measured by the detector. The detection system can take many forms depending upon the parameters being measured. Electrochemical, optical, mass or thermal changes are the most common parameters providing both qualitative or quantitative data.

The sensitivity of biodetectors allows them to be of considerable use as early detection systems against chemical or biological attacks. They are employed to monitor the environment and can respond to low concentrations of any harmful substances that may be present. Biowarfare agents are frequently colourless and odourless and can sometimes take days to cause symptoms. Early detection of these agents is particularly important as they can trigger symptoms, such as fever or nausea that might be initially mistaken for relatively benign conditions like influenza. Biological agents become weapons of mass destruction when they are disseminated through the air as breathable aerosols. Droplets containing the agents can travel through the air over long distances. A healthy human being breathes on average six litres of air per minute and some of the most lethal pathogens are capable of causing disease if as little as ten organisms are inhaled. To be useful as an early warning device, a biodetector must therefore, have a sensitivity that can detect fewer than about two organisms per litre of air.

The biodetectors now under development for use in counterterrorism fall into three broad categories: biochemical systems detecting a DNA sequence or protein unique to the bioagent through interaction with a test

molecule; tissue-based systems, in which a bioagent or toxic chemical affect living mammalian cells, causing them to undergo some measurable response; and chemical mass spectrometry systems, which break samples down into their chemical components whose weights are then compared to those of known biological or chemical agents.

In recent years, researchers have been sequencing the DNA of a number of potential biowarfare agents in an effort to make them available for DNA based biodetector technologies. A microarray of gel-immobilized, fluorescence-labeled nucleic acids has been developed by Argonne National Laboratory. One application of array systems would be to develop a "bacillus microchip" for detecting *Bacillus anthracis* (the anthrax agent). It would distinguish *B. anthracis* from other related bacteria, such as *B. thuringiensis*, *B. subtilis*, and *B. cereus* and also indicate whether the organism is alive or dead by detecting DNA when there are no RNA matches.

A number of new, fast, reliable, and portable DNA detection devices have been developed that can prepare and test samples within a very short time. Devices consisting of cell disruptors, capable of breaking bacterial spores and extracting DNA, which is then used to identify the species of organism, are being tried. Some companies have incorporated an automated sample preparation scheme and coupled it with a microfluidic "lab on a chip" device for detecting microorganisms on the basis of their DNA sequence. The system is said to reduce a laboratory preparation procedure that can take six hours to just 30 minutes. The chip contains tiny channels, valves, and chambers through which milliliters of sample can be pumped and concentrated into a microliter volume. Any bacterial cells are broken ultrasonically and their DNA is extracted, amplified by PCR (polymerase chain reaction) and sequenced.

A DNA-based biochip designed by Northwestern University detects DNA sequences that are specific for pathogenic microorganisms. The chip initially contains very short single strands of DNA between two small electrodes. The DNA strands are complementary to DNA sequences from a specific pathogen. When DNA from that pathogen comes into contact with the chip, it hybridizes with the DNA on the chip. To detect the hybridization, further pieces of DNA are added to the system and these are complementary to the sections of pathogen DNA that have not hybridized. The additional DNA pieces contain gold particles that, on successful hybridization, form a bridge of conducting metal linking the two electrodes. The bridge completes an electrical circuit which raises an alarm.

#### ■ FURTHER READING:

##### PERIODICALS:

- Behnisc, P.A. "Biodetectors in Environmental Chemistry: Are We at a Turning Point?" *Environ Int* 27(2001):441-2.  
Casagrande, R. "Technology against Terror." *Scientific American*. 287 (2002):59-65.

"Early Warning Technology." *Med Device Technol* 13 (2002): 70-2.

##### SEE ALSO

*Biological and Toxin Weapons Convention*  
*Biological Warfare*  
*Biological Warfare, Advanced Diagnostics*  
*Biological Weapons, Genetic Identification*  
*Biosensor Technologies*  
*Chemistry: Applications in Espionage, Intelligence, and Security Issues*  
*Forensic Science*  
*Isotopic Analysis*  
*Microbiology: Applications to Espionage, Intelligence and Security*  
*Molecular Biology: Applications to Espionage, Intelligence and Security Issues*

## Bio-Engineered Tissue Constructs

For several decades, scientists have cultured individual cells and single layers of cells in media outside the body. Information on cell growth, function, and pathology has accumulated from studying these tissue cultures. Very recently, the technology for growing three-dimensional cultures, called tissue engineered constructs (TCE), has evolved. This new technology relies on growing tissues in low gravity fields, in the presence of tissue-specific scaffolding or in highly precise flow or tension environments. The disciplines of biology, physics, and engineering are combined in this new field of tissue engineering (TE). Successful TCE have been used to treat bone disease, replace cartilage and tendons and to repair fascia in hernias. Though there are still many technical problems that must be solved, one of the ultimate goals of TE is to engineer entire organs and to implant them in patients to replace diseased tissues.

Military interest in ETC focuses on using engineered tissue to study and perhaps cure diseases associated with bioterrorism threats. For example, the development of organs that simulate the immune system provide an excellent clinical model on which new vaccines that provide better defense against bioterrorism agents may be tested. Alternatively, artificially engineered lymph nodes or other organs of the immune system could eventually be implanted in humans, inducing a powerful immune response against such biological agents as anthrax, plague, smallpox and other viruses.

In 2002, the Defense Advance Research Projects Agency (DARPA) announced an Engineered Tissue Constructs Program providing funding to research and private institutions to study ETC. The project has two stages. The first is to demonstrate that stem cells can be differentiated into a variety of different types of immune cells within a

three-dimensional tissue construct. Funds for this stage have already been awarded. The second stage is a continuation of the first in which successful tissue engineered constructs are validated for appropriate immune responses.

#### ■ FURTHER READING:

##### BOOKS:

Lanza, Robert P., Robert Langer, and Joseph P. Vacanti. *Principles of Tissue Engineering*. Academic Press, 2000.

##### ELECTRONIC:

Defense Advanced Research Projects Agency, Defense Sciences Office <<http://www.darpa.mil/dso/thrust/biosci/etc.htm>> (March 3, 2003).

Astrom Biosciences, Inc., 24 Frank Lloyd Wright Drive, Ann Arbor, MI 48105. <<http://www.astrom.com>> (March 3, 2003).

Sciperio, Inc., 5202-2 N. Richmond Hill Road, Stillwater, OK 74075. <<http://www.sciperio.com/bio.html>> (March 3, 2003).

The Regional Medical Physics Department of the United Kingdom's National Health Service. "Tissue Engineered Synthetic Scaffolds." <[http://www.rmpd.org.uk/research/bioengineering/tissue\\_engineered\\_synthetic\\_scaffolds.htm](http://www.rmpd.org.uk/research/bioengineering/tissue_engineered_synthetic_scaffolds.htm)> (March 3, 2003).

##### SEE ALSO

*Biological Warfare*  
*Bioterrorism*  
*Smallpox*  
*Vaccines*

## Bio-Flips

Bio-flips are specialized microprocessors that can be implanted in the body and that are capable of configuring and calibrating themselves internally via biological feedback (e.g., a response to a set of biological conditions or parameters). Bio-flip type microprocessors can also be used in external biosensors through which bodily fluids or gases are passed.

The advantage of bio-flip technology is that such microprocessors allow accurate, real-time monitoring of specific physiological processes. For example, one class of bio-flip microprocessors are being designed to take small samples of fluids, analyze those samples, digitize the data, and report results to an external monitor. Bio-flip microprocessors that are capable of monitoring bodily process also offer the potential to allow fine control of these processes.

The United States Department of Defense currently funds research into bio-flip technology because of the potential uses in the monitoring of drug and hormone levels that are often critical in treatment of disease and

injury. Such dynamic implants would, for example, allow more rapid and precise regulation of medication levels at the site of injured tissues. It is anticipated, however, that the widest potential usage of bio-flip technology will be in the development of new drugs and other pharmacogenetic applications. Bio-flip technology also holds the potential to improve genetic testing.

As of 2002, a wide variety of fixed-assay or passive chips are utilized in biosensor technology. Because these passive chips are not capable of reconfiguration or self-recalibration they are often rendered inaccurate when subjected to biological extremes. For example, passive microprocessors are often incapable of yielding accurate biosensor data because of either a deviation from the normally expected baseline function (e.g., the normal or baseline level of a particular gas in the blood) or in situations where there is an excess of a particular substance (e.g., a chemical present in far greater quantities than normally expected).

Microprocessors that can reconfigure and recalibrate will also enhance the accuracy of microarrays utilized for DNA analysis and of biosensors currently capable of performing chemical analysis via capillary electrophoresis or other microfluidic analysis (examination of small samples of fluids).

The task of analyzing massive amounts of data generated by DNA microarrays is often daunting. Bio-flip technologies along with specialized algorithms and specialized computer programs offer scientists hope of improved abilities to detect variation in genetic structure. Accordingly, improvement in bio-flip like microprocessors should improve genotype analysis and improve identification of more DNA biomarkers (e.g., single nucleotide polymorphisms (SNP)) that can be used in determining genetic relatedness, disease susceptibility risk, and the effectiveness (efficacy) of drug treatments.

Advances in bio-flip microprocessors depend on advances in both microprocessor design and microfabrication technology.

##### SEE ALSO

*Biodetectors*  
*Bio-Engineered Tissue Constructs*  
*Biological and Biomimetic Systems*  
*Biological Input/Output Systems (BIOS)*  
*Biological Warfare, Advanced Diagnostics*  
*Biological Weapons, Genetic Identification*  
*Biomedical Technologies*  
*Bio-Optic Synthetic Systems (BOSS)*  
*Biosensor Technologies*  
*Chemical and Biological Detection Technologies*  
*DNA Fingerprinting*  
*DNA Recognition Instruments*  
*Genomics*  
*Microchip*  
*Nanotechnology*  
*Pathogen Genomic Sequencing*  
*Polymerase Chain Reaction (PCR)*  
*Telemetry*  
*Tissue-Based Biosensors*

## Biological and Biomimetic Systems

■ JUDYTH SASSOON

Animals depend on a variety of adaptations and behaviors for reacting to their environment including locomotion, navigation, and the compilation of sensory input into recognizable patterns. The success of these various behaviors is determined by an animal's fitness, which is defined in evolutionary terms as the number of offspring that live to reach reproductive age. Among other effects, these adaptations and behaviors may increase the amount of food an animal forages; increase the number of mates an animal has; or decrease the number of predators an animal encounters. These strategies, which animals have developed through evolutionary pressures, are ideal for incorporation into military systems that navigate, maneuver, sense, analyze, and respond to complex environments.

The Defense Advance Research Projects Agency (DARPA) of the United States government supports a program called Controlled Biological and Biomimetic Systems, whose goal is to incorporate biological evolutionary strategies into new animals or robots that can detect and report the presence of environmental dangers. Some of the applications of the program include developing the capability for mapping the concentration and distribution of toxins within the air, land or water in real time; gathering information on environmental conditions in inaccessible locations or using biological organisms to make the environment more hospitable for troops. The program's aims are entirely defensive. Both private corporations and public laboratories and institutions have been awarded grants within the program.

There are currently three major thrusts of research in the Controlled Biological and Biomimetics Systems program. The goal of the vivisystems program is to exploit live animals, in particular insects, as sentinels for reporting on environmental dangers, including biological weapons. The hybrid biosystems program focuses on developing neural probes that can be used to extract sensory information from animals, in particular insects. The objective of the biomimetics program is to synthesize the biomechanics, neural systems and materials found in organisms for the use in robotic systems.

### ■ FURTHER READING:

#### ELECTRONIC:

Defense Advanced Research Projects Agency, Defense Sciences Office <<http://www.darpa.mil/dso/thrust/biosci/etc.htm>> (March 11, 2003).

Controlled Biological Systems <<http://www.darpa.mil/dso/thrust/biosci/cbs/index.html>> (March 11, 2003).

### SEE ALSO

*Biodetectors*  
*Bio-Engineered Tissue Constructs*  
*Biological Input/Output Systems (BIOS)*  
*Biological Warfare*  
*Biological Warfare, Advanced Diagnostics*  
*Bio-Optic Synthetic Systems (BOSS)*  
*Biosensor Technologies*

## Biological and Toxin Weapons Convention

■ K. LEE LERNER

The Biological Weapons Convention (also more properly, but less widely known as the Biological and Toxin Weapons Convention) is an international agreement that prohibits the development and stockpiling of biological weapons. The language of the Biological Weapons Convention (BWC)—drafted in 1972—describes biological weapons as “repugnant to the conscience of mankind.”

According to the United States Bureau of Arms Control, as of December, 2003, there were 147 countries that were parties to the Biological Weapons Convention. An additional 16 countries were listed as signatory countries who had signed but not yet ratified the BWC.

The BWC broadly prohibits the development of pathogens—disease causing microorganisms such as viruses and bacteria—and biological toxins that do not have established prophylactic merit (i.e., no ability to serve a protective immunological role), beneficial industrial use, or use in medical treatment.

The United States renounced the first-use of biological weapons and restricted future weapons research programs to issues concerning defensive responses (e.g., immunization, detection, etc.), by executive order in 1969.

Although the BWC disarmament provisions stipulated that biological weapons stockpiles were to have been destroyed by 1975, most Western intelligence agencies openly question whether all stockpiles have been destroyed. Despite the fact that it was a signatory party to the 1972 Biological and Toxin Weapons Convention, the former Soviet Union maintained a well-funded and high-intensity biological weapons program throughout the 1970s and 1980s that worked to produce and stockpile biological weapons including anthrax and smallpox agents. U.S. intelligence agencies openly raise doubt as to whether successive Russian biological weapons programs have been completely dismantled. In June, 2002, traces of biological and chemical weapon agents were found in Uzbekistan on a military base used by U.S. troops fighting

in Afghanistan. Early analysis dates and attributes the source of the contamination to former Soviet Union or successive Russian biological and chemical weapons programs that utilized the base.

Evidence of continued biological weapons development and use in Iraq and Iran—both BWC signatory countries—became widely evident during their war in the 1980s. In the wake of the Gulf War, evidence of Iraqi development of prohibited biological weapons mounted throughout the 1990s. Although some weapons were subsequently destroyed by United Nations mandate, in January 2003 the United States Secretary of State Colin L. Powell presented to the United Nations Security Council alleged evidence of Iraq's continued development of prohibited biological weapons.

As of February, 2003, intelligence estimates compiled from various agencies provide indications that more than two dozen countries are actively involved in the development of biological weapons. The U.S. Office of Technology Assessment and the United States Department of State have identified a list of potential enemy states developing biological weapons. Such potentially hostile nations include Iran, Iraq, Libya, Syria, North Korea, and China.

The BWC prohibits the offensive weaponization of biological agents (e.g., anthrax spores). The BWC also prohibits the transformation of biological agents with established legitimate and sanctioned purposes into agents of a nature and quality that could be used to effectively induce illness or death. In addition to offensive weaponization of microorganisms and/or toxins, prohibited research procedures include the concentrating a strain of bacterium or virus, altering the size of aggregations of potentially harmful biologic agents (e.g., refining anthrax spore sizes to spore sizes small enough to be effectively and widely carried in air currents), producing strains capable of withstanding normally adverse environmental conditions (e.g., disbursement weapons blast), and/or the manipulation of a number of other factors that make biologic agents effective weapons.

Although there have been several international meetings designed to strengthen the implementation and monitoring of BWC provisions, BWC verification procedures are currently the responsibility of an ad hoc commission of scientists. Broad international efforts to coordinate and strengthen enforcement of BWC provisions remains elusive.

#### ■ FURTHER READING:

##### BOOKS:

- Cole, Leonard A. *The Eleventh Plague: The Politics of Biological and Chemical Warfare*. New York: WH Freeman and Company, 1996.
- Dando, Malcolm. *Biological Warfare in the 21st Century*. New York: Macmillan, 1994.
- Roberts, Brad. *Biological Weapons: Weapons of the Future?* Washington, D.C.: Center for Strategic and International Studies, 1993.

##### PERIODICALS:

- DaSilva, E., "Biological Warfare, Terrorism, and the Biological Toxin Weapons Convention." *Electronic Journal of Biotechnology*. 3(1999):1–17.
- Dire, D. J., and T. W. McGovern. "CBRNE—Biological Warfare Agents." *eMedicine Journal* 4(2002):1–39.

##### ELECTRONIC:

- United States Department of State. "Parties and Signatories of the Biological Weapons Convention" December 11, 2002. <<http://www.state.gov/t/ac/bw/fs/2002/8026.htm>> (February 25, 2003).

##### SEE ALSO

- Biological Warfare*  
*Biological Warfare, Advanced Diagnostics*  
*Biological Weapons, Genetic Identification*  
*Bioterrorism, Protective Measures*  
*USAMRIID (United States Army Medical Research Institute of Infectious Diseases*  
*Vozrozhdeniye Island, Soviet and Russian Biochemical Facility*  
*World War I*

---

## Biological Input/Output Systems (BIOS)

---

The Biological Input/Output Systems program, also called BIOS, was funded by the Defense Advance Research Projects Agency (DARPA) in 2002. Its goal is to develop and incorporate specific genes into plants, bacteria, yeasts, and prokaryotes that will induce these organisms to act as remote sentinels indicating the presence of biological and chemical substances. These "plug and play" sequences of DNA represent an important step in the development of technology that allow for the assembly of engineered biological pathways within living organisms. For example, an engineered receptor on the exterior of a cell's surface that binds a biological toxin and then signals another pathway within the organism so that it turns different color, activated a fluorescent protein, synthesized a gene product or rearranged a segment of DNA is of particular interest to BIOS. The project aims to produce proof-of-concept examples within three years of initial funding.

An example of a project funded under the BIOS program involves embedding canine olfactory genes that are used in detecting TNT along with the DNA that codes for the pheromone sensing pathway into a yeast's DNA. The potential result is a genetically engineered yeast that can detect explosives. Eventually, these biological sentinels will be grown on sheets that can be deployed in the field.

Another BIOS project focuses on engineering new molecular pathways that result in pigment changes in bacteria upon exposure to a variety of bacterial and viral pathogens. A separate project seeks to engineer biological circuits in the *E. coli* bacterium for sensing biological agents based on the well-known *lac* and *mal* operons as models.

#### ■ FURTHER READING:

##### ELECTRONIC:

Defense Advanced Research Projects Agency, Defense Sciences Office <<http://www.darpa.mil/dso/thrust/biosci/etc.htm>> (March 11, 2003).

##### SEE ALSO

*Biodetectors*  
*Bio-Engineered Tissue Constructs*  
*Biological and Biomimetic Systems*  
*Biological Warfare*  
*Biological Warfare, Advanced Diagnostics*  
*Bio-Optic Synthetic Systems (BOSS)*  
*Biosensor Technologies*

## Biological Warfare

■ JUDYTH SASSOON

Biological warfare, as defined by the United Nations, is the use of any living organism (e.g. bacterium, virus) or an infective component (e.g., toxin), to cause disease or death in humans, animals, or plants. In contrast to bioterrorism, biological warfare is defined as the “state-sanctioned” use of biological weapons on an opposing military force or civilian population. Biological weapons include pathogenic viruses, bacteria, and biological toxins. Of particular concern are genetically altered microorganisms, which are engineered to target a specific group of people.

### Early History of Biological Warfare

Examples of the use of biological weapons exist in ancient records. In the sixth century B.C., Assyrians poisoned enemy wells with ergot, a toxin derived from mold that grows on rye. Other records of battles document the use of diseased corpses to poison wells. In 1346, plague-infected corpses and carcasses were catapulted into Kaffa, a city in current day Crimea, by the Tartar army. The epidemic that resulted may have eventually led to the great Black Plague that afflicted Europe. In 1710, the Russian army used a similar military strategy when it invaded Sweden. The Spanish are reported to have contaminated French wine with blood taken from people suffering from



Chemical/biological warfare agent R400 aerial bombs, destroyed by the United Nations weapons inspectors after the 1991 Persian Gulf War, are seen at the Muthanna State Establishment in Iraq in 1998. AP/WIDE WORLD PHOTOS.

leprosy in the mid-1400s. In the seventeenth century, a Polish general filled artillery shells with the saliva from rabid dogs.

Smallpox was used as a biological weapon several times during the colonization of the Americas. The Spanish explorer Pizarro gave blankets infested with the virus to natives in South America in the fifteenth century. Sir Jeffery Amherst presented blankets contaminated with the smallpox virus to native Americans during the French and Indian war between 1754 and 1767. The epidemic that followed resulted in the surrender of a strategic fort to the English. A Southern doctor is reported to have sold clothing contaminated with smallpox to the Union Army during the Civil War.

### Modern History of Biological Warfare

During the twentieth century, modern scientific methods led to the development, refinement, and stockpiling of weapons of biological warfare by governments throughout the world. During World War I, Germany developed a

biological warfare program based on the bacterium *Bacillus anthracis* and a strain of *Pseudomonas* known as *Burkholderia mallei*, which causes glanders disease in cattle. Dr. Anton Dilger, a German agent living in Washington D.C., reportedly grew anthrax and glanders bacteria in his home and then inoculated thousands of horses and cattle that were shipped to Allied troops in Europe. Many of the animals perished and hundreds of the troops exposed to these animals were secondarily infected by the diseases.

During World War II, prisoners in German Nazi concentration camps were infected with pathogens, such as Hepatitis A, *Plasmodia* spp., and two types of *Rickettsia* bacteria, during studies allegedly designed to develop vaccines and antibacterial drugs. A large reservoir in Bohemia was poisoned with sewage by the German army in 1945.

Between 1918 and 1945, the Japanese government conducted extensive biological weapon research at Unit 731 in occupied Manchuria, China. Prisoners of war were infected with a variety of pathogens, including *Neisseria meningitidis* (meningitis), *Bacillus anthracis* (anthrax), *Shigella* spp. (shigellosis), and *Yersinia pestis* (black plague). Estimates are that over 3,000 prisoners died as a result of infection by these biological pathogens or execution following such infections. In 1941, the Japanese released an estimated 150 million potentially plague-infected fleas from aircraft over cities in China and Manchuria. After these infectious agents were released, outbreaks of plague occurred in many Chinese villages. In addition, approximately 10,000 illnesses and 1,700 deaths occurred among Japanese troops.

Driven by reports of Japanese and German programs to develop biological weapons, the Allies embarked on vigorous efforts to develop their own biological weapons during World War II. Britain produced five million anthrax cakes at the UK Chemical and Biological Defense Establishment at Porton Down with the intent of dropping them on Germany to infect the food chain. These weapons were never used. British open-air testing of anthrax weapons in 1941 on Gruinard Island in Scotland rendered the island inhabitable for five decades.

The United States government's biological warfare facility was headquartered at Fort Detrick in Maryland beginning in 1942. Weapons were also tested and produced in Colorado, Arkansas and Utah. Many different agents were studied including the bacteria that cause anthrax, plague, botulism, Q fever, and staphylococcal infections. Several viruses were also included in the research. The U.S. Army conducted a study in 1951–1952 called "Operation Sea Spray" to study wind currents that might carry biological weapons. As part of the project design, balloons were filled with *Serratia marcescens* (then thought to be harmless, but easily identifiable) and exploded over San Francisco. Shortly thereafter, there was a corresponding dramatic increase in reported pneumonia and urinary tract infections in the region.

The former Soviet Union was implicated in several incidents involving the development and release of biological agents. In 1979, an accidental release of a small amount of anthrax spores occurred at a bioweapons facility near the Soviet city of Sverdlovsk. At least 77 people were sickened and 66 died. All the affected people were some 4 kilometers downwind of the facility. Sheep and cattle up to 50 kilometers downwind became ill. Immediately following the incident, the Soviet government declared that the cause of the illnesses was contaminated meat. However, in 1992 Russian President Boris Yeltsin took responsibility, stating that the accident was the result of military research at the microbiology facility. Between 1975 and 1983, Soviet forces allegedly used "yellow rain" in military operations in Laos, Cambodia and Afghanistan. This substance, T2 toxin or trochothecene mycotoxin, is derived from the *Fusarium* fungi and is extremely damaging to the intestinal tract. The Soviet government has denied the use of T2 toxins, claiming that the yellow rain was the result of defecating bees.

In 1991, the Iraqi government admitted the existence of a biological weapons program within their military. They built bombs containing the botulinum toxin, anthrax and aflatoxins. Iraqi scientists also studied the uses of wheat cover smut, ricin and the toxins produced by *Clostridium perfringens* for biological weapons.

**Diplomacy and biological warfare.** The first diplomatic effort to limit biological warfare was the Geneva Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare. This treaty, ratified in 1925, prohibited the use of biological weapons; however, it was not effective as Germany, the United States, Britain, and the Soviet Union all had biological weapons programs up to the 1960s. More than 140 countries, including the United States, signed the Convention on the Prohibition of the Development Production, and the Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction, also called the Biological Weapons Convention (BWC) in 1972, with limited success. Although the United States formally stopped biological weapons research in 1969 (by executive order of then President Richard M. Nixon), the Soviet Union carried on biological weapons research until its demise. Despite being a signator to the BWC, the Iraqi government allegedly continued its buildup of biological weapons into the twenty-first century.

Following the Iraqi war, however, anticipated stockpiles of biological weapons were not immediately found.

#### ■ FURTHER READING:

##### ELECTRONIC:

Rhode Island Department of Health: Bioterrorism Preparedness Program "History of Biological Warfare and Current Threat" <<http://www.healthri.org/environment/biot/history.htm>> (March 12, 2003).

Arizona Department of Health Services: Epidemiology and Surveillance "History of Biowarfare and Bioterrorism" <<http://www.hs.state.az.us/phs/edc/edrp/es/bthistor2.htm>> (March 12, 2003).

#### SEE ALSO

*Anthrax Weaponization*  
*Biological and Toxin Weapons Convention*  
*Bioterrorism*  
*Chemical Warfare*  
*Infectious Disease, Threats to Security*  
*Viral Biology*  
*Weapons of Mass Destruction*

---

## Biological Warfare, Advanced Diagnostics

---

The Advanced Diagnostics Program is funded by the Defense Advanced Research Projects Agency of the United States government (DARPA). Its objective is to develop tools and medicines to detect and treat biological and chemical weapons in the field at concentrations low enough to prevent illness. Challenges to this task include minimizing the labor, equipment, and time for identifying biological and chemical agents.

One area of interest includes development of field tools that can identify many different agents. To accomplish this goal, several groups funded under the advanced diagnostics program have developed field-based biosensors that can detect a variety of analytes including fragments of DNA, various hormones and proteins, bacteria, salts, and antibodies. These biosensors are portable, run on external power sources, and require very little time to complete analyses.

A second focus of the advanced diagnostics project is the identification of known and unknown or bioengineered pathogens and development of early responses to infections. Many viruses act by destroying the ability of cells to replicate properly. One group funded under the advanced diagnostics program is studying the enzyme 5'-monophosphate dehydrogenase (IMPDH), which produces products that are required for synthesizing nucleic acids, such as RNA and DNA, both of which are essential for proper cell replication. This group seeks to develop novel drugs based on IMPDH, which can cross into cells and thwart viral infection.

A final goal is to develop the ability to continuously monitor the body for evidence of infection. Researchers are addressing this goal in two ways. The first involves engineering monitoring mechanisms that are internal to the body. In particular, groups funded under the initiative are developing bioengineered white blood cells to detect infection from within the body. Often genetic responses to infection occur within minutes of infection so analysis of

blood cells provides a very quick indication of the presence of a biological threat. The second method involves the development of a wearable, non-invasive diagnostic device that detects a broad-spectrum of biological and chemical agents.

#### ■ FURTHER READING:

##### ELECTRONIC:

Advanced Diagnostics (DARPA) <<http://www.darpa.mil/dso/thrust/biosci/ADVDIAG/index.html>> (March 13, 2003).  
 Defense Advanced Research Projects Agency, Defense Sciences Office <<http://www.darpa.mil/dso/thrust/biosci/advdiagn.htm>> (March 13, 2003).

#### SEE ALSO

*Biodetectors*  
*Biological Warfare*  
*Biomedical Technologies*  
*Biosensor Technologies*  
*Bioterrorism*  
*Bioterrorism, Protective Measures*

---

## Biological Weapons, Genetic Identification

---

Biological weapons are weapons whose payload consists of microorganisms that can cause infections, or the toxic components of the microorganisms. Examples of microorganisms include viruses (e.g., smallpox, Ebola, influenza), bacteria (e.g., *Bacillus anthracis*, *Clostridium botulinum*, *Yersinia pestis*) and protozoa. The most prominent example of a toxic component is the variety of toxins produced and released from bacteria (e.g. neurotoxins produced by *Clostridium*).

Genetic technologies can be useful in the detection of biological weapons. Of particular note is the polymerase chain reaction, or PCR, which uses select enzymes to make copies of genetic material. Within a working day, a target sequence of genetic material can be amplified to numbers that are detectable by laboratory tests such as gel electrophoresis. If the target sequence of nucleotides is unique to the microorganism (e.g., a gene encoding a toxin), then PCR can be used to detect a specific microorganism from among the other organisms present in the sample.

Hand-held PCR detectors that have been used by United Nations inspectors in Iraq during their weapons inspections efforts of 2002–2003 purportedly can detect a single living *Bacillus anthracis* bacterium (the agent of anthrax) in an average kitchen-sized room.



The sequence of components that comprise the genetic material (genome) of a microorganism can also be deduced using techniques such as electrophoresis. Once a sequence is known, it can be compared to the many bacterial, viral, protozoal, and other microbial sequences in databases, in order to determine if the deduced sequence resembles a catalogued sequence. In this way, the nature and identity of biological weapons can be determined.

Genetic engineering has also made possible the splicing of the genetic determinants for a lethal agent from one microorganism or other life form into another microbe. For example, the former Soviet Union experimented with the instillation of the gene responsible for the production of cobra toxin into normally harmless bacteria that reside in the intestinal tract.

While recent events in the United States and in other countries, in particular Iraq, have brought biological weapons into prominence, the military use of biological weapons is centuries old. The bloated bodies of disease victims were routinely dumped into wells to poison the drinking water, or were even catapulted over the walls of fortified cities that were under siege.

More recently, biological warfare was an accepted part of the military campaigns of governments around the world. During World War I, for example, Germany actively explored the weaponization of *Bacillus anthracis* and *Burkholderia mallei*. The latter causes Glanders disease in cattle. Its use was intended to cripple the agriculture base of the enemy.

During World War II, Britain also intended to cripple German agriculture by airdropping discs (or cakes) of anthrax. Indeed, five million anthrax cakes were ultimately produced, although they were not used. Also during this war, German and Japanese prisoners were used as guinea pigs in the testing of microbial weapons, including hepatitis A, *Plasmodia* species, *Rickettsia*, *Neisseria meningitis*, *Bacillus anthracis*, *Shigella* species, and *Yersinia pestis*. The U.S. had an active biological weapons program during World War II, and extending even into the 1960s. This program was finally terminated in 1968 by the order of then president Richard Nixon.

The production of biological weapons can be accomplished with relatively unsophisticated microbiological technology and by a typically trained microbiologist. Furthermore, the equipment necessary to accomplish weaponization (i.e., incubators, autoclaves, fermenters, centrifuges, refrigerators, and lyophilizers) can be housed in only a few thousand square feet. Thus, biological weapons manufacture is not difficult to conceal.

Furthermore, while biological weapons can be deployed in traditional weaponry (i.e., rockets), the weapons can also be literally carried in someone's pocket to the target site. This can make the deployment of biological weapons virtually impossible to stop, unless the carrier passes near an instrument designed to detect the biological agent.

Microorganisms are very light and so can be dispersed easily in air currents. This is especially true for bacterial spores, which, when dried, are powdery in texture. Furthermore, because exposure to only a few spores can be sufficient to cause disease (e.g., the inhalation form of anthrax, which is caused by spores of *Bacillus anthracis*), the biological weapon can be easily delivered to the target. The anthrax-containing letters that were mailed in the United States in the latter part of 2001 attest to the ease of delivery.

*Bacillus anthracis* and *Clostridium botulinum* are two prominent examples of spore-forming bacteria that have been used as bioweapons. Spore forming bacteria normally grow and reproduce as "vegetative" cells. But, in harsh environmental conditions that threaten the survival of the bacteria, the microbes have evolved the ability to transform into an almost dormant form known as a spore. The spore is surrounded by a resilient coat that allows it to persist for decades, perhaps even centuries. When conditions again become favorable for growth and reproduction, the spore resuscitates into the vegetative form. Thus, if spore biological weapons do not kill immediately, the residual spores can persist to cause illness many years later.

The microbial agents used as biological weapons are typically highly infectious. The direct exposure of even a small number of people to the weapon can quickly lead to a large number of illnesses or casualties. Bacteria such as *Clostridium botulinum* and various species of *Salmonella* readily cause contamination, either by their growth in food or by the production of potent toxins. Such food-borne microbial threats are also considered to be biological weapons. Indeed, in the aftermath of the U.S. anthrax attacks in 2001, the vulnerability to sabotage of the food production and supply systems in many countries has become evident.

Ironically, the features that make biological weapons attractive to those who wage war or terrorism, namely their ease of dispersal, particularly via air, and their infectivity, has also proved to be a stumbling block to their use. A shift in the prevailing wind can carry the lethal payload back to those who deployed it, similar to the chemical warfare casualties that occurred during World War I. For example, the open air testing of anthrax on Gruinard Island off of the coast of Scotland in 1941 made the island inhabitable for decades afterwards. In a second example, as part of the U.S. Army's "Operation Sea Spray" in 1951–1952, balloons filled with *Serratia marcescens* were exploded over San Francisco, to evaluate the effectiveness of aerial biological warfare on a major urban center. The organism, which up until then was thought to be innocuous, allegedly produced an increase of pneumonias and urinary tract infections in the citizens of the city. As a final example, an accidental release of anthrax spores from a bioweapons facility in 1979 killed 66 people and sickened over 70 who were 4 kilometers downwind, in the city of Sverdlovsk, in the former Soviet Union. Sheep and cattle up to 50 kilometers downwind became ill.

## ■ FURTHER READING:

### BOOKS:

Cirincione, Joseph, Jon B. Wolfsthal, Miriam Rajkuman, and Jessica T. Mathews. *Deadly Arsenals: Tracking Weapons of Mass Destruction*. Washington, D.C.: Carnegie Endowment for International Peace, 2002.

Hamzah, Khidr Ald Al-Abbis, and Jeff Stein. *Saddam's Bombmaker: The Terrifying Inside Story of the Iraq Nuclear and Biological Weapons Agenda*. New York: Scribner, 2002.

Lavoy, Peter R., Scott D. Sagan, and James J. Wirtz. *Planning the Unthinkable: How New Powers Will Use Nuclear, Biological, and Chemical Weapons*. Cornell University Press, 2001.

### SEE ALSO

*Anthrax Weaponization*

*Biocontainment Laboratories*

*DNA*

*Infectious Disease, Threats to Security*

*Pathogens*

---

## Bio-Magnetics

---

In 2002, the Defense Advance Research Projects Agency (DARPA) funded an initiative to research the use of magnetic technologies in the detection, manipulation and control of cells, molecules and nanomolecules called Bio-Magnetics Interfacing Concepts (BioMagnetICs). Living cells and biological molecules are not particularly polar, therefore using magnetic markers as tags represents a highly specific and easily detectable signal for measuring cellular response to environmental conditions, including the presence of biological and chemical toxins. The function of cells and tissues are, to a large extent, managed by the flow of chemical information across membranes via membrane receptor molecules. These membrane receptors are extremely specific, controlling exactly which molecules pass in and out of the cell and at what rate. DARPA's bio-magnetics program seeks to exploit these molecular functionalities by building stable, accurate and sensitive sensors that detect and monitor cellular functions such as protein synthesis, DNA expression, cell death and pigment generation.

The BioMagnetICs program has three major goals. First, it hopes to develop new magnetic tags, or ferrofluids, which have a strong magnetic signal and which can be attached to specific cells and biological molecules. Second, research within the BioMagnetICs program will focus on developing highly sensitive magnetic tags for attachment to fragments of molecules with diameters less than 100 nm within living cells. The final objective of the BioMagnetICs program is to develop magnetic tweezers that can manipulate single molecules and fragments of molecules with precision on the order of nanometers.

One of the expected technologies resulting from the BioMagnetICs program includes bio-detection devices that can detect several different analytes very quickly and with minimal preparation of samples. These magnetic readers have the capacity to provide 10 to 1000 times more sensitivity than is possible using current analysis techniques. In addition, these devices are expected to detect toxins with a specificity that is greater than 99%. Because biological and chemical toxins can be dangerous in extremely low concentrations, speed, sensitivity and specificity are extremely important for ensuring the safety of troops in regions where weapons of mass destruction may play an important role.

## ■ FURTHER READING:

### ELECTRONIC:

Defense Advanced Research Projects Agency, Defense Sciences Office <<http://www.darpa.mil/dso/thrust/biosci/biomagn.htm>> (March 20, 2003).

### SEE ALSO

*Biodetectors*

*Biological Warfare*

*Biological Warfare, Advanced Diagnostics*

*Biosensor Technologies*

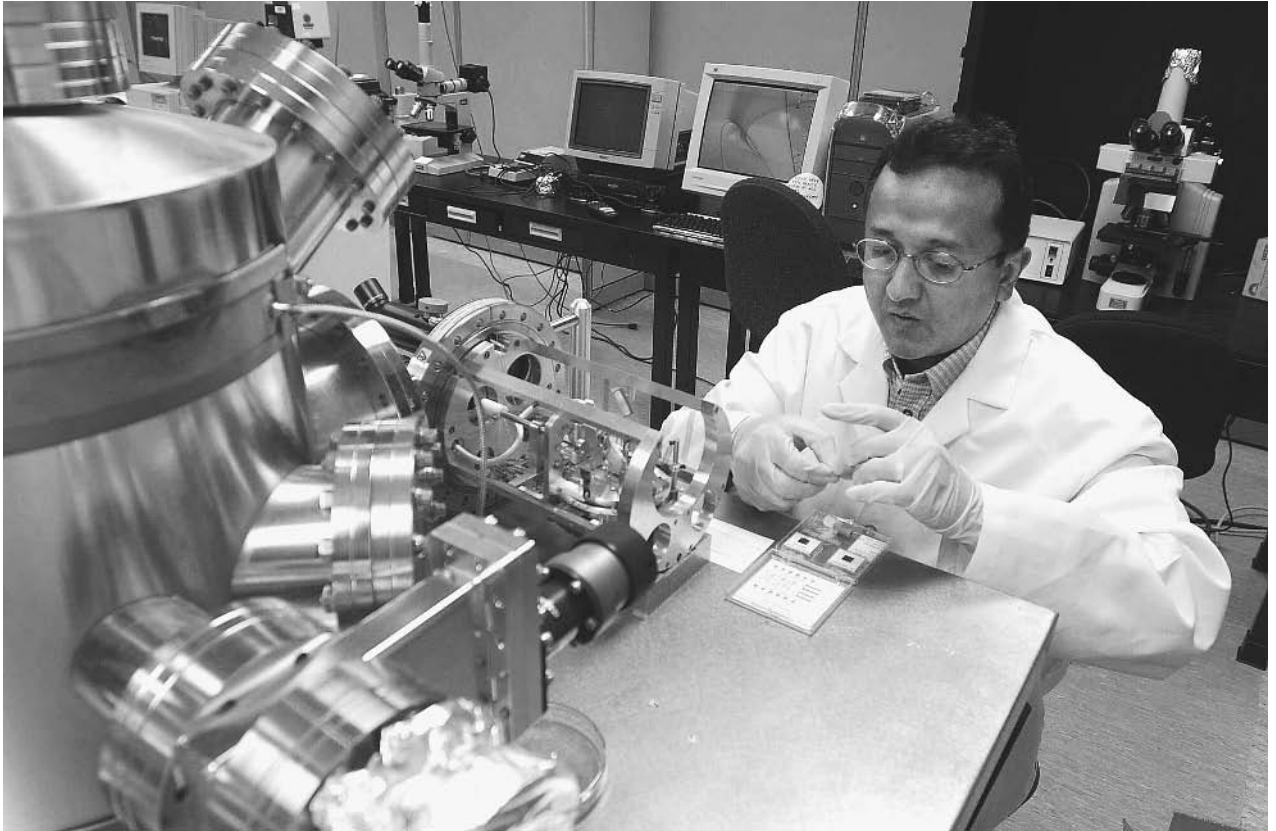
---

## Biomedical Technologies

---

In 1993, the Defense Advance Research Projects Agency (DARPA) initiated a program to develop biomedical technologies for use on the front line of the battlefield in 1993. Research had shown that even though medical care has greatly improved during the last three decades, the number of casualties on the battlefield has essentially remained constant. The focus of the Advanced Biomedical Technologies Program (ABMT) was to apply techniques in robotics, virtual reality, three-dimensional visualization, telesurgery, microelectromechanical systems (MEMS), informatics and multi-media simulation to producing products for the care of wounded personnel on the front lines of war. Achievements were made in each of the projects three major research areas: diagnostics, therapeutics, and education and training.

ABMT developed several technologies to improve diagnosis of wounded soldiers on the battlefield, including a Personal Status Monitor (PSM) that continuously monitors vital signs and location and reports this information to medical units. When a soldier is injured, medical personnel can quickly detect his or her location and the seriousness of the wounds. In the near future, troops will wear smart tee shirts, which will have sensors woven into



A Purdue University professor demonstrates an atomic force microscope, used to view biochips, a technology aimed at making diagnostic devices that can be used to quickly analyze samples with high sensitivity. AP/WIDE WORLD PHOTOS.

the fabric that monitor and transmit vital signs and location to medics in real-time. ABMT has also developed hand-held sensors for taking ultrasounds, measuring blood gases and body chemistry, and producing digital pathology reports in the field.

ABMT has also developed new therapeutic technologies for use on the front lines. The Life Support for Trauma and Transport (LSAT) unit is a commercially available stretcher that performs all of the functions of a portable intensive care unit. Medics evacuate wounded soldiers to LSAT units where they can administer IV fluids, intubate and ventilate lungs, and medicate and monitor the soldier until they reach a hospital unit. In addition, ABMT developed several systems for performing telesurgery in remote locations using telemedicine, robotics, and miniaturization.

The final focus of AMBT was to develop novel educational and training tools for troops. Virtual reality (VR) programs simulate battlefield situations and give soldiers first-hand experience for assessing the status of a wounded soldier and deciding on the best way to diagnose, treat, and evacuate the injured individual. Multi-media simulations teach an array of surgical and medical techniques focusing on the procedures that medics are most likely to encounter on the front lines of the battlefield.

#### ■ FURTHER READING:

##### ELECTRONIC

Defense Advanced Research Projects Agency, Defense Sciences Office "Advanced Biomedical Technologies" <<http://www.darpa.mil/dso/trans/abt.htm>> (March 24, 2003).

##### SEE ALSO

*DARPA (Defense Advanced Research Projects Agency)*

## Biometrics

#### ■ K. LEE LERNER

Biometrics refers to the measurement of specific physical or behavioral characteristics and the use of that data in identifying subjects. With wide application, biometric-based identification techniques are increasingly an important part of physical and financial security infrastructure because biometric data is difficult, if not impossible, to

duplicate or otherwise falsify. Accordingly, biometric systems offer highly accurate means of comparison of measured characteristics to those in a preassembled database.

Biometric identification points include gross morphological appearance that is most often subjectively interpreted upon superficial examination (e.g., gender, race or color of skin, hair and eye color). Other gross biometric data can include more quantifiable—and therefore less subjective—data (e.g., weight, height, location of scars or other visible physical markings).

Some biometric data are easily changeable and therefore not reliable (e.g. presence of facial hair, wearing of glasses, etc.).

Because even objective features such as weight can change over time, systems of identification that rely on changeable or gross features are not as reliable as biometric systems that measure more stable anatomical and physiological characteristics such as fingerprints, retinal blood vessel patterns, specific skull dimensions; dental and skeletal x-rays, earlobe capillary patterns and hand geometry.

The most specific and reliable of biometric data are obtained from DNA sequencing.

More controversial and, at present, less reliable biometric studies seek to enhance quantification of social behaviors, voice characteristics—including language use patterns and accents—handwriting and even keystroke input patterns.

Biometric data can be encoded into magnetic stripes, bar codes, and integrated circuit “smart” cards.

On a global scale, biometric data interchange and interoperability standards are at present fragmented into different measurement and input format schemes. The Common Biometric Exchange File Format (CBEFF), in development by the International Biometric Industry Association (IBIA), seeks to integrate such measurement schemes to enhance reliability and use of biometric data. Other integration efforts include the Biometric Application Programming Interface (BioAPI) specification program used by the United States Department of Defense. The Department of Defense has also established a Biometrics Management Office (BMO). BioAPI protocols are also being used by other governmental agencies and the financial service industry in the development of smart cards.

In the private sector, specific organizations regulate need-driven biometric integration schemes. For example, the American National Standards Institute (ANSI) establishes specific biometric standards for the financial industry.

One system already with broad integration is used by the American Association for Motor Vehicle Administration (AAMVA). The Driver’s License and Identification (DL/ID) standards are used to provide rapid and accurate identification based upon data gathered during the issuance of a driver’s license within Canada or the United States.

The National Institute of Standards and Technology (NIST) also has programs dedicated to biometric research and exchange. NIST developed the initial data protocols

used in the Face Recognition Vendor Test (FRVT) and established the format for data collection used by most face recognition technologies.

## ■ FURTHER READING:

### BOOKS:

Jain, A., A. Bolle, and S. Pankanti. *Biometrics, Personal Identification in Networked Society*. Norwell, MA: Kluwer Academic Publishers, 1999.

### PERIODICALS:

Podio F., et al. “Common Biometric Exchange File Format (CBEFF).” *NISTIR 6529* (January 3, 2000).

### ELECTRONIC:

NIST Biometric Interoperability, Performance and Assurance Working Group (May, 2003) <<http://www.nist.gov/bcwg>> (May, 10, 2003).

### SEE ALSO

*APIS (Advance Passenger Information System)*

*Closed-Circuit Television (CCTV)*

*Facility Security*

*Fingerprint Analysis*

*Forensic Voice and Tape Analysis*

*IBIS (Interagency Border Inspection System)*

*IDENT (Automated Biometric Identification System)*

*INSPASS (Immigration and Naturalization Service Passenger Accelerated Service System)*

*Los Alamos National Laboratory*

*NAILS (National Automated Immigration Lookout System)*

*NIST (United States National Institute of Standards and Technology)*

*PORTPASS (Port Passenger Accelerated Service System)*

*Retina and Iris Scans*

*SENTRI (Secure Electronic Network for Travelers’ Rapid Inspection)*

---

## Bio-Optic Synthetic Systems (BOSS)

---

In 2002, the Defense Advanced Research Project Agency (DARPA) initiated a program aimed at simplifying complex optical sensors used in military operations by imitating biological visual systems. The goal of the Bio-Optical Synthetic Systems project (BOSS) is to understand and synthesize the components of biological vision systems.

Much of the current technology used for intelligence gathering depends on optical sensors. These sensors are complicated, relying on multiple sets of lenses for focusing on their targets. Biological vision systems, such as the

eye, are extremely compact, yet allow for a wide field of view, a dynamic range of index of refraction and control over spherical aberration. The crystalline structure of the fish eye lens, for example, accomplishes this flexibility in optical properties via an inhomogeneous protein gradient.

The technical challenges for this project include developing materials with a dynamic index of refraction and a variable field of view lens. In particular, the program specifies that the lens must have a field of view ranging from less than one degree to 120 degrees. The program seeks to develop material to improve the index of refraction, which likely requires the use of an inhomogeneous protein gradient. Materials that self-assemble into such hierarchical structure are of key interest. Both public institutions and private corporations have been funded under this initiative.

#### ■ FURTHER READING:

##### ELECTRONIC:

Defense Advanced Research Projects Agency, Defense Sciences Office "Bio-Optic Synthetic Systems (BOSS)" <<http://www.darpa.mil/dso/thrust/biosci/boss.htm>> (March 25, 2003).

##### SEE ALSO

*Biodetectors*  
*Bio-Engineered Tissue Constructs*  
*Biological and Biomimetic Systems*  
*Biosensor Technologies*  
*Brain-Machine Interfaces*  
*DARPA (Defense Advanced Research Projects Agency)*

## Biosensor Technologies

The capability for detecting and identifying multiple biological warfare agents quickly and accurately is required to protect both troops on the battlefields and civilians confronted with terrorist attacks. The systems currently available for sensing biological analytes rely on two technologies: reporter molecules that attach to antibodies and give off fluorescent signals and the Polymerase Chain Reaction (PCR) that amplifies suspect DNA. Because two steps are required to identify biological weapons, the procedure is both labor and time intensive. The Defense Advanced Research Projects Agency (DARPA) initiated the Biosensor Technologies Program in 2002 to develop fast, sensitive, automatic technologies for the detection and identification of biological warfare agents. The program focuses on a variety of technologies including surface receptor properties, nucleic acid sequences, identification of molecules found on the breath, and mass spectrometry.

A major thrust of the surface receptor research is to enhance or replace the signal given off by antibodies to biological analytes. One such project has developed short polypeptides (4–5 amino acids long) that can bind to anthrax spores. A separate group has engineered aptamers, short strands of nucleic acid that specifically bind to the DNA of the bacteria that cause anthrax. Another research area involves using ion channels for amplifying the signal of a reporter molecule. This work includes the engineering of an artificial ion channel that is triggered by the binding of an antibody or other small molecules. Such engineered ion channels are sensitive to a single binding event, require no external energy and can greatly amplify the chemical signal. Finally, upconverting phosphors as a replacement for fluorescent reporter molecules are being investigated.

The focus of the nucleic acid sequence technology is the development of a biochip that contains an array of engineered molecules that react with the genome of biological warfare agents. The biochip is embedded in a platform that is portable, automated and allows for direct sampling of the environment. A biochip platform to identify the anthrax bacteria is in the testing stages and additional biochips for identifying other harmful bacteria and viruses are in development.

#### ■ FURTHER READING:

##### ELECTRONIC:

Defense Advanced Research Projects Agency: Defense Sciences Office <<http://www.darpa.mil/dso/thrust/biosci/biotech.htm>> (March 26, 2003).

Biosensor Technologies <<http://www.darpa.mil/dso/thrust/biosci/biosensor/index.html>> (March 11, 2003).

##### SEE ALSO

*Anthrax*  
*Biodetectors*  
*Biological Input/Output Systems (BIOS)*  
*Biological Warfare, Advanced Diagnostics*  
*DARPA (Defense Advanced Research Projects Agency)*

## BioShield Project

#### ■ JULI BERWALD

Although the medical industry has made great strides in the treatment of many naturally occurring diseases, such as cancer and heart disease, over the last few decades, very little has changed in the treatment of many of the diseases that might be used in a terrorist attack. In

particular, the smallpox vaccine has not changed much since the 1960s and the treatments for exposure to radiation have remained the same since the 1970s. The goal of the BioShield project is to focus biomedical research and development on the field of bioterrorism to improve the treatment of bioterrorism threats.

President George W. Bush announced Project BioShield during his State of the Union Address in January of 2003. As approved by Congress, this project commits \$6 billion to improve treatment of diseases caused by biological, chemical and radiological weapons. The project is a joint effort between the Department of Homeland Security and the Department of Health and Human Services.

Under the BioShield Project, resources will be made available to buy the most effective drugs and vaccines available for the treatment of anthrax, smallpox, and botulism and, in the future, ebola and plague. This financial commitment is intended to ensure that the private sector produces the vaccines and drugs required to treat bioterrorist threats. The Secretary of Health and Human Services will identify the most critical threats and will collaborate with industry to develop and make available the most effective countermeasures.

The project gives the National Institute of Health funding to expedite research into the most promising new drug treatments. In particular, procedures to speed up the funding process for grant proposals for research into new drug therapies for chemical, biological and radiological diseases will be authorized. Technical experts will be hired more quickly and equipment required for research will be purchased more rapidly. There is hope that some of the most recent research in the fields of genetics, immunology, molecular engineering and proteomics will be useful in developing novel treatments for the diseases caused by bioterrorism. In addition, some of the innovations developed under Project BioShield may become important in the treatment of naturally occurring diseases.

The BioShield project provides the Food and Drug Administration with the authority to make promising drugs widely available in emergency situations.

#### ■ FURTHER READING:

##### ELECTRONIC:

Defense Advanced Research Projects Agency: Defense Sciences Office <<http://www.darpa.mil/dso/thrust/biosci/biotech.htm>> (March 26, 2003).

The White House, News & Policies. President Details Project BioShield. February 3, 2003. <<http://www.whitehouse.gov/news/releases/2003/02/20030203.html>> (April, 3 2003).

##### SEE ALSO

*Anthrax*  
*Biological Warfare*  
*Biological Warfare, Advanced Diagnostics*

## Bioterrorism

■ BRIAN HOYLE

Bioterrorism is the use of a biological weapon against a civilian or military population by a government, organization, or individual. As with any form of terrorism, its purposes include the undermining of morale, creating chaos, or achieving political goals. Biological weapons use microorganisms and toxins to produce disease and death in humans, livestock, and crops.

Bioterrorism is viewed as a serious threat to national security. For example, disaster scenarios created by United States government agencies predict that the release of a few hundred pounds of the spores of *Bacillus anthracis* (the bacterium that cause the disease called anthrax) upwind of Washington, D.C., could sicken or kill hundreds of thousands to millions of people within twenty-four hours.

Bioterrorism can also be used as a weapon to damage or destroy the economy of the target nation. A report from the Centers for Disease Control and Prevention estimates the costs of dealing with a large-scale anthrax incident is at least \$26 billion per 100,000 people. Only a few such incidents could cripple the economy of any nation. Indeed, the few anthrax incidents in the last few months of 2001 cost the United States government hundreds of millions of dollars in treatment, investigation, and other response measures.

Biological, chemical, and nuclear weapons can all be used to achieve similar destructive goals (i.e., massive loss of life). In comparison, biological weapons are inexpensive to make, relative to chemical and nuclear weapons. A sophisticated biological production facility can be set up in a warehouse, or even in a building as small as a house. Biological weapons are relatively easy to transport and resist detection by standard security systems.

In general, chemical weapons act immediately, causing illness in minutes. For example, the release of sarin gas in the Tokyo subway in 1995 by the religious sect Aum Shinrikyo almost immediately killed 12 and hospitalized 5,000 people. In contrast, the illness and death from biological weapons can occur more slowly, with evidence of exposure and illness appearing over time. Thus, a bioterrorist attack may at first be indistinguishable from a natural outbreak of an infectious disease. By the time the deliberate nature of the attack is realized, the health care system may be unable to cope with the large number of victims.

The deliberate production and stockpiling of biological weapons is prohibited by the 1972 Biological Weapons Convention. The United States ceased offensive production of biological weapons in 1969, on orders from then President Richard Nixon. The U.S. stockpiles were destroyed in 1971–1972. This measure has not stopped



University of Nebraska researchers explain laboratory automation equipment available to analyze bioterrorism agents to the Secretary of the Department of Homeland Security, Tom Ridge, second from right. AP/WIDE WORLD PHOTOS.

bioterrorists from acquiring the materials and expertise needed to produce biological weapons.

Genetic engineering can produce a wide variety of bioweapons including bacteria or viruses that produce toxins. More conventional laboratory technologies can also produce bacteria that are resistant to antibiotics.

Examples of the most likely to be used bioterrorist weapons include smallpox (caused by the Variola virus), anthrax (caused by *Bacillus anthracis*), and plague (caused by *Yersinia pestis*).

The last recorded case of smallpox was in Somalia in 1977. As of 2002, only two facilities—one in the United States and one in Russia—are authorized to store the virus. In spite of international prohibitions, security experts suspect that smallpox viruses may be under development as biological weapons in other laboratories of many nations. As recently as 1992, Russia had the ability to launch missiles containing weapons-grade smallpox. A number of terrorist organizations including Al Qaeda have explored the use of biological weapons.

Bioterrorism may ultimately prove to be more destructive than conventional warfare, because of the mobility of the weapons and their ability to spread infection

through an entire population. An epidemic can spread a disease far from the point of origin of the illness.

Preparing a strategy to defend against biological warfare is challenging. Traditional identification of microorganisms such as bacteria and viruses relies on assays that detect growth of the microbes. Newer technologies detect microbes based on sequences of genetic material. The genetic technologies can detect microbes in minutes. As of 2002, however, the genetic technologies are not available to any but the most sophisticated field investigative units.

Researchers are also working to counter bioterrorist attacks using several other new technological strategies. For example, robots equipped with sensors or microchip-mechanized insects (with computerized circuitry that can mimic biological processes such as neural networks) are being developed. Bees, beetles, and other insects outfitted with sensors are used to collect real-time information about the presence of toxins or similar threats. These new technologies could be used to examine a suspected biological weapon and spare exposing investigators to potential hazards. The robotics program of the Defense Advanced Research Project (DARPA) works to rapidly identify bio-responses to pathogens, and for designs to effectively and rapidly treat them.

Research is also underway to find genetic similarities between the microbes that could be used by bioterrorists. A vaccine made of a protein that is common to several bacteria could potentially offer protection to the exposure any bacterium in the group, for example.

#### ■ FURTHER READING:

##### BOOKS:

Frist, W.H. *When Every Moment Counts: What You Need to Know about Bioterrorism from the Senates only Doctor*. Lanham, MD: Rowman & Littlefield, 2002.

Henderson, D. A., and T. V. Inglesby. *Bioterrorism: Guidelines for Medical and Public Health Management*. Chicago: American Medical Association, 2002.

Inglesby, Thomas V. "Bioterrorist Threats: What the Infectious Disease Community Should Know about Anthrax and Plague," in *Emerging Infections 5* Washington, D.C.: American Society for Microbiology Press, 2001.

##### PERIODICALS:

Kaufmann, A.F., M.I. Meltzer, and G.P. Schmid. "The Economic Impact of a Bioterrorist Attack: Are Prevention and Postattack Intervention Program Justifiable?" *Emerging Infectious Diseases* no. 3 (1997): 83–94.

##### SEE ALSO

*Anthrax, Terrorist Use as a Biological Weapon*  
*Anthrax Vaccine*  
*Anthrax Weaponization*  
*Antibiotics*  
*Biocontainment Laboratories*  
*Biological Warfare*  
*Biological Warfare, Advanced Diagnostics*  
*Biological and Toxin Weapons Convention*  
*Biological weapons, Genetic Identification*  
*Bioterrorism, Protective Measures*  
*Chemical and Biological Defense Information Analysis Center (CBIAC)*  
*Chemical and Biological Detection Technologies*  
*Chemical and Biological Incident Response Force, United States*  
*DARPA (Defense Advanced Research Projects Agency)*  
*DNA Recognition Instruments*  
*DNA Sequences, Unique*  
*Mail Sanitization*  
*Pathogen Genomic Sequencing*  
*Pathogen Transmission*  
*Pathogens*  
*Polymerase Chain Reaction (PCR)*  
*Salmonella and Salmonella Food Poisoning*  
*Smallpox Vaccine*  
*Spores*  
*Weapons of Mass Destruction*  
*Weapons of Mass Destruction, Detection*  
*World War I*

## Bioterrorism, Protective Measures

■ K. LEE LERNER

Bioterrorism is the deliberate use of microorganisms or the poisonous compounds that can be produced by some microbes as weapons. Bioterrorism can be a well-organized government sanctioned weapons development program, or can involve a small group of people dedicated to their particular cause.

In the past, the weapons employed by nations were more easily recognizable and defendable. For example, surveillance allows missile silos to be detected, and counter-strategies put in place to deal with the launch of the missiles. Microorganisms, however, by virtue of their small size can be readily hidden from detection. A vial of anthrax spores—small enough to conceal in a pocket—can be released into the ventilation system of a building.

The ability to protect against the use of biological weapons is becoming recognized as one of the paramount security issues facing nations such as the United States.

The need for protective measures against bioterrorism was dramatically evident in the aftermath of the September 11, 2001 terrorist attacks on the United States, when a lethal form of the anthrax bacterium that could be inhaled was mailed to U.S. government leaders, media representatives, and citizens. The form that readiness and response strategies should take is the subject of much public debate.

A range of protective options exist. These include the mass production and stockpiling of antibiotics (i.e., ciprofloxacin, which is normally effective against the bacterial agent of anthrax) and the resumption of offensive biological weapons programs by countries such as the United States (where offensive research was halted in 1968). However, no single solution will provide protection against the many potential biological weapons. Indeed, an argument has been made that a targeted response (e.g., broadly inoculating the public against the virus causing smallpox) might actually lower overall preparedness by diverting personnel and funding from fundamental research programs that could help spawn a variety of protective measures.

The various protective measures to bioterrorism can be divided into three general categories. These are strategic, tactical, and personal measures.

Strategic deterrence can involve international cooperation. For example, late in 2001, the United States and NATO (North Atlantic Treaty Organization) allies reaffirmed treaty commitments that the use weapons of mass destruction (i.e., biological, chemical, or nuclear weapons) against any member state would represent an attack against all NATO members. As of June 2002, this deterrence was pointed at states—in particular Iraq—that have



programs to develop or use biological weapons, or which provide aid to bioterrorists.

Tactical measures involve the use of devices or weapons to detect or eliminate potential biological weapons. The United States has a variety of tactical non-nuclear options, which include precision-guided conventional thermal fuel-air bombs. In the 1990s military campaigns in the Gulf region, for example, these bombs were used to destroy facilities that were suspected of being factories for the production of biological warfare agents and weaponry.

Terrorist operations are enigmatic and elusive. As a result, these large-scale military responses offer protection against only the largest, identifiable, and targetable enemies. Such responses are inadequate when the hostility is due a small number of people operating in a clandestine way in other countries, or even citizens targeting their own country. For example, according to expert testimony before the Congress, for less than 10,000 U.S. dollars, a laboratory capable of producing spores of the anthrax bacterium could be built in the basement of a typical house. Surveillance of every structure in a country is beyond the scope of established security agencies and, in a democratic country, would severely curtail individual liberties.

Reestablishing offensive weapons programs is a contentious issue. An argument has been made that an offensive program would further the understanding of potential biological agents and weapons delivery mechanisms. However, many scientists and physicians argue instead that an offensive program is unneeded and could possibly be detrimental to the development of effective protective measures, because of the diversion of funding from less visible but vital preventative research. Resumption of an offensive bioweapons programs in the United States would violate the Biological Weapons Convention to which the United States is a signatory.

Rather than a polarized offensive-versus-preventative national policy, scientific bodies in the United States that include the National Institutes of Health and the Centers for Disease Control and Prevention (CDC) advocate a balanced and flexible scientific and medical response to the need to develop protective measures against the variety of disease causing pathogens in the arsenal of the bioterrorist.

Preparedness programs designed to allow a rapid response to bioterrorism also accompany the increased research. One example is the National Pharmaceutical Stockpile Program (NPS). The NPS stockpile of antibiotics, vaccines, and other medical treatment countermeasures is can be rapidly deployed to the site of a domestic attack. For example, in the aftermath of the deliberate release of *Bacillus anthracis* (the bacteria that causes anthrax) during the 2001 terrorist attacks, the United States government and some state agencies were able to quickly provide the antibiotic ciprofloxacin (Cipro) to those potentially exposed to the bacterium.

Following these bioterrorist attacks, increase funding for the NPS was authorized. The additional funds will help train medical personnel in the early identification and treatment of disease caused by the most likely pathogens.

Such steps are commendable, but will not provide comprehensive and effective protection to biological terrorism. Indeed, such protection may not be possible.

Advocates of increased research capabilities argue that laboratory and hospital facilities must be increased and modernized to provide maximum scientific flexibility in the identification and response to biogenic threats. The CDC has already established a bioterrorism response program that includes increased testing and treatment capacity. The plan also envisions an enhanced ability to recognize and respond to the illness patterns that are characteristic of the deliberate release of an infectious agent.

An informed and watchful public is a key element in early detection of biological pathogens. Knowing this, the CDC web site contains a list of potential biological threats. As of July 2002, approximately 36 microbes had been identified (e.g., Ebola virus variants, plague bacterium, etc.) as potential bioterrorist weapons.

Other protective and emergency response measures include the development of the CDC Rapid Response and Advanced Technology laboratory, a Health Alert Network (HAN), National Electronic Data Surveillance System (NEDSS), and Epidemic Information Exchange (Epi-X). These responses are designed to coordinate information exchange to enhance the early detection and identification of biological weapons.

The United States Department of Health and Human Services 1999 Bioterrorism Initiative committed funds to initiate or reinforce some of these protective measures. Following the September 11, 2001 terrorist attacks on the United States, the U.S. Congress more than doubled the previous funding for bioterrorism research. Soon thereafter, the Bioterrorism Preparedness and Response Program (BPRP) was created. The BPRP seeks to increase the number and capacity of laboratories that are capable of identifying pathogens and developing countermeasures to their use.

An essential component of a preventative response including effective therapeutic treatments is basic research into the biology and disease mechanisms of the disease causing microorganisms. In response to terrorist attacks, in February 2002, the U.S. National Institute of Allergy and Infectious Diseases (NIAID) undertook a review of current research efforts. The panel of experts convened for this task hopes to recommend research thrusts that will more effectively anticipate and counter potential terrorist threats. An immediate outcome of the panel's deliberations was an increased emphasis on basic research involving smallpox, anthrax, botulism, plague, tularemia, and viral hemorrhagic fevers.

In addition to medical protective measures, a terrorist biological weapon attack targeted at humans would, at a

minimum, overburden medical infrastructure. Medical personnel and supplies would be in short supply. As well, the costs of responding to attacks would cause economic havoc. Alternatively, a biological weapon that spared humans but targeted domestic animals or crops could cause famine and economic ruin.

On a local level, cities and communities are being encouraged to develop specific response procedures in the event of bioterrorism. Most hospitals are now required to have response plans in place as part of their accreditation requirements.

Another aspect of prevention focuses on the drinking water supply of communities. Many microorganisms or their poisons readily dissolve in water, and so can be spread to a population virtually undetected. As well, water supplies and distribution systems have been designed for efficiency of water disinfection and delivery, not for security. Because of this, many communities have placed extra security on water supply and treatment facilities. The U.S. Environmental Protection Agency (EPA) has increased monitoring and working with local water suppliers to develop emergency response plans.

It is beyond the scope of this article to discuss specific personal protective measures. Indeed, given the complexities and ever-changing threat, it would not be prudent to offer such specific medical advice. However, a number of general issues and measures can be discussed. For example, military surplus gas masks provide only the illusion of protection. They offer no real protection against biological agents, and should not be bought for that purpose. Personnel stockpiling of antibiotics is unwise. The potency of antibiotics such as Cipro declines with time. Moreover, the inappropriate use of antibiotics actually can lead to the development of bacterial resistance and a consequential lowering of antibiotic effectiveness.

On the other hand, a few days supply of food and water and the identification of rooms in homes and offices that can be temporarily sealed with duct tape to reduce outside air infiltration is a wise precaution.

More specific response plans and protective measures are often based upon existing assessments of the danger posed by specific diseases and the organisms that produce the disease. For example, Anthrax (*Bacillus anthracis*), Botulism (*Clostridium botulinum* toxin), Plague (*Yersinia pestis*, Smallpox (*Variola major*, Tularemia (*Francisella tularensis*, viral hemorrhagic fevers (e.g., Ebola, Marburg), and arenaviruses (e.g., Lassa) are considered high-risk high-priority. These agents do share a common trait of being easily spread from person to person. And, they all can kill many of those who are infected. But, the natures of the diseases they cause are very different. A response that is effective against one microorganism may well be useless against another.

The protective measures that are in place against smallpox and anthrax remain controversial. Vaccines against both diseases are available. However, both vaccines carry the risk of serious side effects. In the absence of

a confirmed case of smallpox, the CDC's position is that the risks of resuming general smallpox vaccination outweigh the potential benefits. Vaccine is available for use in a bioterrorist emergency, when the benefits of mass vaccination could well outweigh the risks of harm due to the vaccine. Moreover, vaccines delivered and injected during the incubation period for smallpox (approximately 12 days) convey at least some protection from the ravages of the disease.

Also controversial remains the safety and effectiveness of an anthrax vaccine used primarily by military personnel.

#### BOOKS:

Henderson, D.A., and T.V. Inglesby. *Bioterrorism: Guidelines for Medical and Public Health Management*. Chicago: American Medical Association, 2002.

Inglesby, Thomas V. "Bioterrorist Threats: What the Infectious Disease Community Should Know about Anthrax and Plague." *Emerging Infections* 5 Washington, D.C.: American Society for Microbiology Press, 2001.

#### ELECTRONIC:

World Health Organization. "Strengthening Global Preparedness for Defense against Infectious Disease Threats." Statement to the United States Senate Committee on Foreign Relations Hearing on The Threat of Bioterrorism and the Spread of Infectious Diseases. 5 September 2001. <[http://www.who.int/emc/pdfs/Senate\\_hearing.pdf](http://www.who.int/emc/pdfs/Senate_hearing.pdf)> (24 November 2002).

#### SEE ALSO

*Anthrax, Terrorist Use as a Biological Weapon Biological Warfare*  
USAMRIID (United States Army Medical Research Institute of Infectious Diseases  
*Vaccines*

## Black Boxes.

SEE *Flight Data Recorders*.

---

## Black Chamber

---

■ DAVID TULLOCH

The term "black chamber" has come to represent any code-breaking organization, but was originally applied to groups of code-breakers associated with the French postal service that intercepted, read, copied and decoded diplomatic mail. In the twentieth century, Americans created a black chamber to intercept and decode radio transmissions (telegraphs) rather than postal mail.

In the seventeenth century, talented individuals such as Antoine Rossignol (1600–1682) in France, and John Wallis (1616–1703) in England showed the value of code breakers in affairs of state. Their efforts encouraged European governments in the eighteenth century to recruit further generations of cryptologists, and create formal cryptology organizations that took their collective title from the French *cabinet noir* (“black chamber”). Usually located within post office buildings, the members of the black chamber would carefully open the sealed mail, make copies of suspect passages, and close the letters with forged wax seals. Then the laborious task of deciphering coded communications would begin.

Most of Europe’s black chambers were closed in the mid-nineteenth century by a combination of public opinion and new social philosophies. The reading of other people’s mail was seen as an infringement of personal freedom. In England public pressure forced the government to cease its opening of diplomatic mail in 1844. Four years later, the black chambers of Austria and France also ended their work.

America did not have a black chamber until the early twentieth century, and it was concerned with radio transmissions (telegraphs) rather than postal mail. Its fame is mainly due to Herbert Osborne Yardley (1889–1958), who described the inner workings of the covert organization in his book, *The American Black Chamber*. Yardley wrote his controversial text after the closing of the code-breaking organization in 1929. The Hoover government wanted to promote trust in international relations, and as Secretary of State Henry Stimson noted, “Gentlemen do not read each other’s mail.” However, by 1940, the black chamber had to be reformed (without Yardley) to counter the threat of war. Today black chambers have become electronic monitoring systems, which many governments use to monitor suspicious communications across the world.

#### ■ FURTHER READING:

##### BOOKS:

Kahn, David, *The Codebreakers: The Story of Secret Writing*. New York, NY: The Macmillan Company, 1967.

Yardley, Herbert O. *The American Black Chamber*. Indianapolis: Bobbs-Merrill, 1931.

———. *The Chinese Black Chamber*, Boston: Houghton Mifflin, 1983.

##### SEE ALSO

*Codes and ciphers*  
*Cryptology, History*  
*Decryption*

## Black List.

SEE *McCarthyism*.

## Black Ops

“Black ops” is shorthand for “black operations,” covert or clandestine activities that cannot be linked to the organization that undertakes them. The term is a highly problematic one, for a number of reasons. First, by definition, many activities conducted by organizations such as the United States Central Intelligence Agency (CIA) are never intended to be linked to the agency itself. Second, a known example of a successful black operation would be a contradiction in terms.

Third, and perhaps most important, is the fact that the term “black ops” itself is much more likely to be used by novices than by members of the intelligence community. A member of the CIA or any such agency would not likely use such a term in describing a true black operation for obvious reasons; agents would be much more likely to disguise the nature of their undertaking with innocuous language. On the other hand, the intriguing sound of the phrase “black ops” makes it highly appealing to conspiracy-theory buffs and others whose interest is more in fantasy than in the often mundane reality of intelligence work. A search of the term “black ops” on the Internet is likely to turn up material from the organizational fringes (some of it tongue-in-cheek), rather than any serious investigation of clandestine activities.

#### ■ FURTHER READING:

##### BOOKS:

Kahaner, Larry. *Competitive Intelligence: From Black Ops to Boardrooms: How Businesses Gather, Analyze, and Use Information to Succeed in the Global Marketplace*. New York: Simon & Schuster, 1996.

Nutter, John Jacob. *The CIA’s Black Ops: Covert Action, Foreign Policy, and Democracy*. Amherst, NY: Prometheus Books, 2000.

##### SEE ALSO

*Covert Operations*

## Black Tom Explosion

#### ■ ADRIENNE WILMOTH LERNER

The Black Tom explosion was the peak act of German sabotage on American soil during the First World War. On July 29, 1916, German agents set fire to a complex of warehouses and ships in the New York harbor that held munitions, fuel, and explosives bound to aid the Allies in



Smoke billowing from the Black Tom explosion, a German sabotage operation on American soil in 1916. ©BETTMANN/CORBIS.

their fight. Though America was technically a neutral nation at the time of the attack, general policies greatly favored the Allies. The attack persuaded many that the United States should join the Allies and intervene in the war in Europe.

**German intelligence and sabotage operations.** As soon as war broke out in Europe, the United States began manufacturing munitions and sharing the weapons with allied British, French, and Russian forces in Europe. German agents in the United States reported the stockpiling and shipping of weapons, and the German government took action. Because they could only openly attack United States property in limited ways such as the sinking of merchant ships carrying contraband munitions without provoking America to wage war, the German government sent undercover agents to sabotage munitions operations. Numerous fires were set at military supply manufacturing sites. Shipping lines and railroads were also sometimes targets. Over 50 acts of sabotage were carried out on American targets from 1914 to 1918. Of those 50, nearly 30 occurred in the New York area alone. Not only did several factories and

warehouses operate in the New York area, but ports in and around New York were the major staging point for shipping supplies to the western front in Europe.

Black Tom pier was located across the harbor from Ellis Island and the Statue of Liberty. The pier partially rested on Black Tom Island, from which it derived its name. The adjacent shore was crowded with warehouses, loading docks, and train tracks. While shipping had always flowed steadily from Black Tom, German agents noted an increase of activity from the site after the outbreak of war. Further investigations revealed that Black Tom was indeed connected to the war effort, and was the major shipping point for most of the fuel reserves bound for Europe. A munitions factory in Manhattan also shipped the detonator fuses it manufactured from Black Tom. A Pennsylvania company used the pier to load dynamite and other explosives onto transports. The combination of materials made Black Tom not only a dangerous place, but also a prime target for sabotage. Destruction of Black Tom would not only stall the shipment of supplies to Europe, but the volatile cargo would ignite and likely cause considerable property damage to the surrounding area.

**Planning the attack at Black Tom.** In 1914, shortly after the start of war in Europe, the German government sent a new ambassador to Washington. Count Johann Von Bernstorff brought with him a consular staff not of diplomats, but of trained German intelligence operatives. The staff also had an unusually high budget of 150 million dollars. The staff performed regular consular duties, but also led a network of other agents in the United States. They designated targets for sabotage, and used their money to buy resources and bribe officials. Soon after the German delegation arrived, the first sabotage fires were reported. In addition to monetary damage, the fires scarred the pre-1920s American psyche. A certain hysteria began regarding the presence of spies and saboteurs on American soil. Rumors of German agents spreading germs, planting bombs, and kidnapping people were plentiful in the public imagination. Even though the threat posed by saboteurs on the public was propagandized to the extreme, the actions of saboteurs were limited in scope until 1916.

German agents, including master spy Franz von Rintelen, worked to increase the damage inflicted by their attacks. Von Rintelen devised an explosive charge called a pencil bomb that was designed to detonate when a ship was already out to sea. German intelligence alerted the German navy of the position and names of ships that were carrying weapons and supplies. Some of these merchant vessels were sunk without warning. After just a few short months, von Rintelen and his operatives caused nearly 100 million dollars worth of damage. British intelligence and police then devised a plan to lure von Rintelen back to Germany via Britain. British intelligence sent the agent a telegram with fake orders from German command to attack a target off the British coastline. Von Rintelen took the bait, was promptly arrested before arriving in Britain, and was extradited back to the United States to stand trial. Sabotage attacks continued to occur. Von Rintelen's most ambitious plan for destruction was carried out in his absence.

**The Black Tom explosion.** Months before his capture, von Rintelen established a team of agents that would be responsible for the destruction of Black Tom Pier. He hired several agents to perform various tasks from smuggling the charges onto ships to bribing pier workers. It remains unknown who actually lit the first explosive fuse to cause the explosion at Black Tom. Police investigations pointed to a man named Michael Kristoff who was living at a boarding house in Bayonne, New Jersey, and was reported by his land lady to keep odd hours and often return home smelling of fuel or having small soot stains on his hands or clothing. Kristoff, when later questioned by authorities mentioned several other accomplices, but did not specifically mention their various roles in the sabotage.

The exact events of the night of the Black Tom explosion largely remain a mystery. Several night watchmen

guarded the area around the pier, but two were later discovered to have accepted bribes from German agents to loosen their guard. The cargo itself was largely unprotected, and sat loaded on moored barges and hips in the harbor. An ammunition storage facility and several fuel tanks were located on the adjacent shore. The first fire and explosion most likely began in this area. Guards fled the scene, wary of the materials they knew were in the vicinity. At 2:08 a.m., a thunderous explosion shook the New Jersey harbor, shattered windows, and threw people from their beds across the bay in Manhattan. That explosion began aboard the *Johnson 17*, a ship carrying explosives and fuel that was docked near the pier. Several other explosions were heard shortly after, and continued until dawn. Shrapnel rained down on New York City and the New Jersey harbor area. Immigrants awaiting entry processing on Ellis Island were evacuated from their barracks, and the Statue of Liberty sustained damage from flying debris. When all of the fuel and explosives were spent, the smoke cleared to reveal a swath of devastation several city blocks wide. Black Tom pier and most of its island were gone.

**Investigation following the war.** Following the war, a special commission convened to assess damages from various incidences of terrorism in the United States. The Mixed Claims Commission consisted of a German, an American, and a neutral representative. The commission reviewed the claims of industries, companies, and governments that lost property to the work of saboteurs during the war. The Black Tom explosion was the largest of such claims. After reviewing evidence supplied by police and intelligence investigations, the panel decided that the explosion was the result of foul play on the part of German terrorists. The commission awarded a settlement amount of 50 million dollars, the largest damage claim awarded for a single incident during the war. The money was to be paid from German reparations payments proscribed in the Treaty of Versailles. The damage award to the plaintiffs, however, was not finally made until 1939.

#### ■ FURTHER READING :

##### BOOKS:

Volkman, Ernest. *Espionage: The Greatest Spy Operations of the Twentieth Century*. New York: John Wiley & Sons, 1996.

Whitcover, Jules. *Sabotage at Black Tom: Imperial Germany's Secret War in America, 1914-1917*. Chapel Hill, NC: Algonquin Books, 1989.

##### ELECTRONIC:

Vogel, Peter. "Ship Explosions: Black Tom Island, SS *Mary Luckenbach*, SS *Robert Rowan*, USS *Mount Hood*" from *The Last Wave from Port Chicago* 2001. <<http://www.portchicago.org/lastwave/chapter8.htm>> (December 2, 2003).

## SEE ALSO

*World War I*

## Bletchley Park

■ ADRIENNE WILMOTH LERNER

Bletchley Park was the headquarters of the British Military Intelligence Government Code and Cipher School during World War II. Located fifty miles north of London, on the grounds of the sprawling Victorian mansion for which it was named, Bletchley Park employed 12,000 code breakers and staff. Bletchley Park cryptologists successfully broke the major codes used by the German military and high command, creating the most advanced computing sources of the time with few resources. British cryptologists also aided United States efforts to break Japanese codes. Intelligence information gathered from Bletchley Park is credited with significantly aiding the Allied war effort and saving thousands of lives.

**The beginning of Bletchley Park.** Although British Military Intelligence employed code breakers during World War I, they failed to establish a permanent cryptology department in the inter-war period. In 1938, on the eve of World War II, British Military Intelligence revived the cryptology department. Drafting cryptographers from all disciplines, and heavily recruiting young men from Oxford and Cambridge, the first cryptology operations were established in London. The group's main task was to correspond with foreign code breakers in allied nations and cull information regarding their cryptology efforts against German codes.

In the summer of 1939, British Intelligence moved the cryptology department to Bletchley Park, officially dubbed Station X because it was the tenth division of the intelligence organization. A cipher school was established on the grounds to train new code breakers. As war was on the horizon, a large number of women were trained for employment at Bletchley Park. At the height of the war, three-quarters of Bletchley Park staff were women. The focus of operations at Station X shifted to active code breaking. By the outbreak of World War II in September of 1939, Bletchley Park cryptologists had already made considerable progress against some German diplomatic codes.

**Early code breaking efforts.** During the two years of the war, British cryptologists decoded German communications with limited success. Older codes, used for low security messages, were readily identified and broken by the Bletchley Park team. Some newer codes were broken mathematically, but decoding and translating these messages by hand proved an arduous task. By the time messages

were fully understood, the information they contained was often outdated. Compounding the problem, these intercepts contained very little useful intelligence information. Since the mid-1930s, the German government had used complex cipher machines to disguise their most important communications.

The first great code breaking triumph at Bletchley Park came on August 30, 1941. A British "Y Station," one of the military listening stations that intercepted German communications, picked up a depth, a repeat transmission that used the same settings on the cipher machine. This intercept was forwarded to Bletchley Park. Cryptologists identified as "fish," the nickname for a message produced by the illusive *Geheimschreiber* cipher machine. Within two months, the Bletchley Park team broke the high-level German code.

To facilitate the processing of "fish" intercepts, Bletchley Park engineers borrowed an idea from plans the Polish intelligence service gave Britain before the war. They constructed a machine that aided the deciphering of intercepts, nicknamed a "bombe" because of the low, roaring noise it made while operating. The "bombe" constructed to decipher *Geheimschreiber* transmissions did help cryptographers to process intercepts more rapidly, but the machine required the exact synchronization of two paper tapes for printing. The tapes often broke, and the machine had to be reset. In addition, the start setting to process each intercept, the original cipher settings used by the Germans to send the message, had to be calculated by British cryptologists by hand. The process was still too complex to yield decoded intercepts ready for immediate translation to be useful to intelligence and military personnel.

**Operation Ultra: breaking the German Enigma machine.** Most of Germany's high-level military messages were encoded using a cipher machine called Enigma. The complex code used not only a cipher, but also an overlaying encryption to disguise the original text. The series of rotor wheels on the Enigma teleprinter gave the machine an extraordinary number of code combinations. The Germans were so confident that the machine code was so nearly infinite in possibilities that it could never be broken. However, various intelligence services in neighboring nations had made considerable progress breaking Enigma even before the outbreak of the war. In Britain, efforts to break Enigma were known as Operation Ultra.

In the months preceding the German invasion of Poland in 1939, Polish intelligence passed on to British intelligence information on their efforts to break Enigma. Most helpful was the information Polish spies gathered on how the cipher machine operated, including sketches of the teleprinter and some of its components. With the information, Bletchley Park cryptologists found two key weak links in the Enigma code. Enigma code prohibited that any letter be encrypted as itself, and German standards of communication dictated that the same phrase



The Duke of York, foreground, reads a printout from the Colossus computer during his tour of Bletchley Park, the former British Spy Center, England. ©CORBIS SYGMA.

begin all transmissions. Exploiting these two weaknesses, British cryptologists unraveled the Enigma code mathematically in late 1940.

Even though cryptologists could read portions of Enigma transmissions, they encountered the same delay of accessing intercepted information as they had with other codes. Another bombe was constructed that could process Enigma codes, expediting code breaking. However, cryptologists and engineers at Bletchley Park realized that another mechanical solution was needed to fully exploit German intercepts. To this end, two Bletchley Park engineers invented Colossus, the first electronic, programmable machine in 1943. Colossus not only decoded messages, but also broke through the overlaying cipher, producing a ready to translate copy of the intercept in the original German. With Colossus, Bletchley Park could decipher German communications before the intended recipients. Translated intercepts were immediately passed on to intelligence and military officials, making Bletchley Park central to the Allied war effort.

**Security at Bletchley Park.** Concerned that the German military and government would change encryption devices if they knew of the operation, operations at Bletchley

Park were shrouded in absolute secrecy. Details of Operation Ultra and other specific code breaking missions were fully known by only four people. A special intelligence protocol was established to funnel information into and out of Bletchley Park. No one link in the chain of information knew more than two other people involved in the operation.

In order to guard Bletchley Park secrets in the event of a German invasion or bombing campaign of Britain, Bletchley Park's extensive archives of every decoded intercept and the accompanying original intercept were photographed and catalogued at the Bodleian Library at Oxford University. Code breaking equipment was supposed to be entirely disassembled, put on a nearby train to Liverpool, and then ferried to the United States if Bletchley Park were in danger of falling into enemy hands. The tight security surrounding Bletchley Park was remarkably successful. The operation was one of the few government and military outposts that was not compromised by German spies.

**Legacy of Bletchley Park.** The work of cryptologists and engineers at Bletchley Park is often credited with shortening the duration of the war in Europe by an estimated two to three years. Bletchley Park intelligence aided military

strategy, the shipment of necessary troops and supplies, and turned the tide of the war in favor of the Allies.

German U-boats controlled the seas until Bletchley Park decoded intercepts provided military leaders and shipping interests with up-to-date fleet positions and mission reports. Ultra intelligence aided the sinking of the German destroyer, *Bismarck*, a great moral victor for the British Navy.

On land, Station X intelligence helped Allied forces plan their invasions of North Africa, Italy, and France. During the D-Day offensive and the subsequent Allied march across France, military field command received daily intelligence updates based on information garnered by Bletchley Park code breaking efforts.

Bletchley Park also intercepted the first dispatches relating to German prisoner of war and concentration camps. Other intercepts decoded by Bletchley Park provided Allied military leaders with the first evidence of the Holocaust.

After the war, the Bletchley Park was abandoned and the staff sworn to secrecy regarding their wartime employment. All of the deciphering equipment, including replica teleprinters, bombs, and even Colossus, were disassembled and archived or simply destroyed. By March of 1946, no trace of Station X operations remained on the grounds of Bletchley Park, with the exception of the hastily constructed outbuildings, known as huts, which housed offices and staff. British Military Intelligence, known after the war as MI-6, did not dissolve the Government Cipher School or cryptology department. The department was moved to MI-6 headquarters in London, and then to Cheltenham in 1952 where its main mission was the decoding of Soviet Cold War-era communications.

Although its contribution to the war effort was highly significant, the exploits of Bletchley Park were not fully known until details regarding Operation Ultra and Station X were finally declassified in 1989. The continued secrecy of Bletchley Park allowed American engineers in 1945 to take credit for the invention of the world's first computer, ENIAC, built two years after Colossus. No member of the Bletchley Park staff betrayed the secrets of Station X until the government opened its files to the public.

#### ■ FURTHER READING :

##### BOOKS:

Hinsley, F. H. *British Intelligence in the Second World War*. Cambridge: Cambridge University Press, 1988.

Hinsley, F. H. and Alan Stripp, eds. *Codebreakers: The Inside Story of Bletchley Park*. Oxford: Oxford University Press, 2001.

Smith, Michael. *Station X: Decoding Nazi Secrets*. London: TV Books, 2000.

##### SEE ALSO

*Codes and Ciphers*

*Codes, Fast and Scalable Scientific Computation*  
*Colossus I*  
*FISH (German Geheimschreiber Cipher machine)*  
*Operation Magic*  
*OSS (United States Office of Strategic Services)*  
*Poland, Intelligence and Security*  
*Ultra, Operation*  
*United Kingdom, Intelligence and security*  
*World War II*

## Bolivia, Intelligence and Security

Bolivia gained its independence from Spain in 1825. Since then, the nation has weathered nearly 200 political coups and other incidences of political upheaval. Throughout the last century, power has shifted between large land-owners and military interests. However, political reforms in the 1980s brought the first democratized government to power. The nation still deals with periodic unrest, but continuing reform policies and an expanding intelligence and security community have helped to stabilize the Bolivian government.

Bolivia's main civilian intelligence branch collects and processes both domestic and foreign intelligence. The Ministry of the Interior oversees government intelligence services, including the Special Security Group and the Multipurpose Intervention Brigade (BIP). Both agencies have garnered criticism from Bolivian citizens and journalists for conducting political espionage operations in recent years.

Illegal drug trafficking remains one of Bolivia's main political and social issues. In cooperation with international anti-crime and anti-trafficking efforts, Bolivia established the Special Anti-narcotics Force (FELCN). The FELCN maintains intelligence personnel and surveillance equipment to identify and track drug smuggling rings. The agency also has elite action units that infiltrate trafficking networks and made arrests. The FELCN also works closely with The Bolivian National Police.

Bolivia's intelligence community has a full-time anti-terrorism department, the Special Elite Anti-terrorism Force (FEAE). This unit has been operational in Bolivia long before the recent international focus on global terrorism. FEAE focuses on collecting intelligence regarding threats to Bolivian national interests and government personnel, mostly from paramilitary groups in Latin America and from drug cartels.

Bolivia is a member of the United Nations (UN) and several pan-Latin American security organizations.



## ■ FURTHER READING:

### ELECTRONIC:

Central Intelligence Agency. "Bolivia" CIA World Factbook <<http://www.cia.gov/cia/publications/factbook/geos/bl.html>> (April 8, 2003).

# Bomb Damage, Forensic Assessment

## ■ JUDSON KNIGHT

Just as fires and explosions are closely related phenomena in physical and chemical terms, bomb-damage assessment is an aspect of forensic science closely related to arson investigation. In both cases, authorities analyze a crime scene for telltale signs of the nature of the materials that facilitated the conflagration. In the United States, the two agencies most concerned with bomb-damage assessment at the federal level are the Bureau of Alcohol, Tobacco, and Firearms (ATF), and the Explosives Unit of the Federal Bureau of Investigation (FBI).

Both fires and explosions involve a physical change in materials, such as the conversion of solid or liquid into gas, as well as the conversion of small quantities of matter into energy. Additionally, these processes involve a chemical change or reaction, that is, a rearrangement of atoms. Both processes must take place in the presence of oxygen, which is among the most reactive of the chemical elements, meaning that it is highly likely to bond with atoms of other elements.

During the process of oxidation, an element bonding with oxygen loses electrons, while the oxygen gains electrons, a process chemically known as reduction. The world is full of oxidation-reduction reactions, some of which include the rusting or corrosion of metals, the metabolism of food and other biological processes, and combustion. The last of these is commonly known as the process by which materials catch fire, and explosion is simply a fast form of combustion. In the combustion process, chemical bonds are broken quickly, releasing energy that is experienced in the form of heat. In the case of explosion, these bonds are broken even more quickly, producing even more heat and more kinetic energy, which propels objects outward from the center of the blast with greater impact.

**Investigating a crime scene.** The investigator of a scene where a bombing has taken place must be schooled both in basic physics and chemistry, but also forensic science, or the application of scientific techniques for the purpose of solving crimes. One of the first matters of interest to the investigator, obviously, is the nature of the explosive itself. At the low end of the spectrum are unsophisticated

devices such as pipe bombs, which are usually little more than metal pipe containing black powder from shotgun shells.

Much more complex are explosives using TNT (trinitoluene) or nitroglycerin. The latter is found in dynamite, which combines sodium nitrate, nitroglycerin, and inert compounds. One notorious variety of explosive is ammonium nitrate, used in the 1993 World Trade Center bombing and the 1995 Oklahoma City bombing. Combined with fuel oil, it is known as ANFO, a foul-smelling—and lethal—sludge.

One difference between lower-level explosives and their more sophisticated cousins is the fact that the latter requires a detonator or blasting cap, a device to make it active. Investigators will, therefore, seek not only the telltale physical and chemical residue that will lead to a determination of the type of bomb used, but also for evidence of detonators and other components such as tapes, wires, timers, switches, and batteries.

**Agencies and bombings.** ATF agents investigating the first World Trade Center bombing, which killed six people, found a great deal of chemical evidence in the aftermath, ranging from the acrid, acidic smell of the air to specific types of molecular residue. There was also physical evidence that identified the perpetrators' van as the site where the blast originated: among the items noted were "feathering," or the fact of being stretched by the blast; "bluing," exposure to welding-torch-like heat; and "dimpling," whereby the metal close to the blast liquefied and shot out, colliding with nearby objects and leaving tiny craters on their surfaces.

In addition to the ATF, the FBI operates a laboratory to which other law-enforcement agencies submit materials for investigation. At the international level, bomb damage assessment may be performed by security services of various nations, or even by international teams, which may include civilians. Such was the case in the investigation of the scene in Bali, Indonesia, where Islamist terrorists detonated a bomb that killed several hundred people in October 2002.

## ■ FURTHER READING:

### BOOKS:

Bolz, Frank, et al. *The Counterterrorism Handbook: Tactics, Procedures, and Techniques*. Boca Raton, FL: CRC Press, 2002.

### ELECTRONIC:

BBC News. Q&A: Bali Forensic Challenge. <<http://news.bbc.co.uk/2/hi/asia-pacific/2327687.stm>> (January 16, 2003).

Bureau of Alcohol, Tobacco, and Firearms. Arson and Explosives Programs. <<http://www.atf.treas.gov/expl arson/index.htm>> (January 16, 2003).



An Australian forensic team collects evidence at the bombing site of a nightclub in Kuta, Bali, that killed nearly 200 people. Suspects arrested for the bombing claimed to be members of the Jemaah Islamiyah regional network, an ally of Osama bin Laden's Al Qaeda. AP/WIDE WORLD PHOTOS.

FBI Laboratory Explosives Unit. <<http://www.fbi.gov/hq/lab/org/eu.htm>> (January 16, 2003).

#### SEE ALSO

*Bomb Detection Devices*  
*Forensic Science*

## Bomb Detection Devices

■ BRIAN HOYLE

When detonated in strategic, population-dense, or confined spaces, bombs are especially destructive. For example, a bomb planted by political terrorists in a suitcase was responsible for the explosion of Pan Am Flight 103 over Lockerbie, Scotland, on December 21, 1988, that claimed 270 lives. Given the devastation that bombs can cause, and the risk they pose to national security, the detection of bombs is a important priority in airports and elsewhere.

Despite the fact that x-ray examination may not detect some bombs, the technique is still a mainstay in bomb detection. For example, x rays are the best way to reveal

the presence in luggage of suspicious shapes. Plastic explosives can be molded to resemble common objects. Also, explosives are not metallic, and so will escape metal detection. A well-trained operator is a key part of this bomb detection strategy. A newer version of the x-ray examination places a reflector on the opposite side of an object from the x-ray beam. As the rays are scattered back, they are analyzed by a sophisticated computer program, which can reveal differences in the outgoing and incoming beams that were caused by passage of the beams through suspicious material.

Another version of the x-ray dual energy technology sends two x-ray beams through the object at the same time. One of the beams distinguishes organic material (i.e., food, leather objects, paper) and displays them as red. The other beam distinguishes inorganic objects (i.e., metal clips, umbrella, metal pens) as green or blue. The color difference helps the operator quickly scan packages and baggage for object that are suspicious by their shape or chemistry. A similar method, which uses radio waves instead of x rays, is called quadrupole resonance technology.

Another optical device is computer tomography, a technique that has been adapted from the CAT scan x-ray technology used in the medical operating room. In



A dust sample is taken from a laptop computer and the particles analyzed for explosives residue by a Barringer explosives detection device. AP/WIDE WORLD PHOTOS.

tomography, an object is scanned and then a computer analyzes the x-ray image. If areas of the package have not been adequately revealed, the x-ray source can be rotated so as to produce a detailed view of the specific area. In this way packages and baggage can be examined in great detail.

Some bomb components can leave a scent. Until a few decades ago, specially trained dogs were a mainstay of bomb detection squads. Specially trained dogs are still used today to check out packages or locations that are difficult to examine using a machine. A dog's nose is actually a bit more sensitive than the sensitivity of detection machinery that is currently available. However, a dog and handler costs approximately \$50,000 a year, whereas a piece of detection equipment represents a one-time cost of \$20,000 to \$40,000. Thus, machines are becoming more prevalent.

One such technology utilizes gas chromatography and a property called chemiluminescence. In gas chromatography, chemicals of different composition can be separated from each other based on their differing speeds in a stream of gas (selection of the gas can determine the rate of movement of different compounds). A compound in the gas, which will then glow, will recognize an isolated compound that has a certain chemical group in its structure. The glowing (chemiluminescence) registers on an optical detector, revealing the presence of the explosive chemical.

Devices known as sniffers detect vapor given off by certain explosives. Chemicals such as nitroglycerin are readily detected. But, a sniffer can miss explosives such as plastic explosives that do not readily vaporize. Thus, a sniffer should be used only as part of a bomb detection regimen that involves other detection techniques.

Another device detects chemicals present in bombs by concentrating the air collected from a target location. The air is drawn through a filter, where explosive chemicals collect, due to their tendency to be heavier than the air molecules around them. The filter is analyzed using ion mobility spectrometry

The spectrometric technique is very sensitive. Less than a nanogram ( $10_9$  of a gram) of explosives residue can be detected. To put this into perspective, a fingerprint on a luggage handle left by someone had been handling explosives will typically contain 100,000 times more of the residue.

#### ■ FURTHER READING:

##### BOOKS:

Green, Michael. *Bomb Detection Squads*. Mankato, MN: Capstone Press, 1998.

Shubert, Hiltmar, Andre Kuznetsov, and Audrey Kuznetsov. *Detection of Explosives and Landmines*. Hingham, MA: Kluwer Academic Publishers, 2002.

Yinon, Jehuda. *Forensic and Environmental Detection of Explosives*. New York: John Wiley & Sons, 1999.

##### ELECTRONIC:

Sandia National Laboratories. "Miniaturization of chemical preconcentrators brings better bomb-detecting and drug-sniffing devices." Sandia Lab News. August 13, 1999. <[http://www.sandia.gov/LabNews/LN08-13-99/sniffer\\_story.html](http://www.sandia.gov/LabNews/LN08-13-99/sniffer_story.html)>(21 January 2003).

##### SEE ALSO

*Explosive Coal*  
*Gas Chromatograph-Mass Spectrometer*  
*Isotopic Analysis*  
*Metal Detectors*  
*Remote Sensing*

## Bombe

#### ■ ADRIENNE WILMOTH LERNER

A bombe was a mechanical device used for the rapid decryption and transcription of complex ciphers. Developed during World War II, the multiple bombes employed by British and United States military intelligence code breakers aided the allied war effort by providing access to German and Japanese military secrets. The most famous bombe, employed by British code breakers at Bletchley



Joe Desch, shown in 1943, headed a top-secret program at the National Cash Register Co. in Dayton, Ohio, to develop a high-speed deciphering machine called a Bombe, used to crack the Nazi submarine code. AP/WIDE WORLD PHOTOS.

Park against the German Enigma cipher, could break messages 72 times faster than the first Pentium computer.

The bombe derived its name from the loud, rhythmic, and somewhat ominous ticking noise it made while computing code permutations. The machine itself was highly complex, requiring skill in mathematical code breaking and engineering to construct. Throughout World War II, the form of the bombe changed many times. Each improvement added to the machine's ultimate effectiveness and efficiency.

**Enigma and the development of the bombe.** Most of Germany's high-level military messages were encoded using a cipher machine called Enigma. The complex code used not only a cipher, but also an overlaying encryption to disguise the original text. The series of rotor wheels on the Enigma teleprinter gave the machine an extraordinary number of code combinations. The Germans were confident that the machine code was perfectly random, and therefore mathematically unbreakable. However, both Polish and Swedish intelligence made significant progress breaking Enigma even before the outbreak of World War II.

In the months preceding the German invasion of Poland in 1939, Polish intelligence gave British intelligence information on their efforts to break Enigma. Most

helpful was the information Polish spies gathered on how the cipher machine operated, including sketches of the teleprinter and some of its components. The Poles also included blueprints for a code-breaking device that they had not yet been able to construct, the first bombe decoder. At the time the Poles broke Enigma using longhand mathematics, the Enigma machine had only three rotors. On the eve of war, the Germans replaced most of the three rotor machines with new a new five rotor model, making Enigma more difficult to break, and sending British engineers back to the drawing board to redesign the bombe.

Before the mechanical device could be designed and constructed, however, Bletchley Park cryptologists had to break the new version mathematically. With the information provided by Polish intelligence, Bletchley Park cryptologists found two key weak links in the Enigma code. Enigma code prohibited that any letter be encrypted as itself, and German standards of diplomatic communication dictated that the same phrase begin many transmissions. Exploiting these two weaknesses, British cryptologists broke Enigma in 1940. Within a year, they had broken two other major German codes, including the perplexing Lorenz cipher used by Hitler's High Command. Bletchley Park engineers then set out to adapt original bombe designs to operate against the new codes.

British engineer Alan Turing designed and constructed the first successful bombe. The Turing Bombe, or "Tabs," as it became known, operated against the German Enigma code, but could be adapted to decipher other codes. The Turing Bombe was the main device used against Enigma, but its complex operation required the work of several operators. During the course of the war, women were the predominant operators of Bletchley Park bombes, decoding and translating intercepts for intelligence service use. Even with the operation of several bombes, Enigma intercept information could not be used in "real time" but military field command or forward intelligence units. A series of improvements aided computational time, including a diagonal switchboard and "machine gun" voltage regulator, which were added to eliminate processing errors that stopped the bombe's computation. A teleprinter was added to the device to allow for simultaneous transcription of messages into the original German, ready for translation.

British intelligence shared some of their cryptanalytic work with United States forces, even before the U.S. entered the war in 1941. However, after the bombing of Pearl Harbor, President Roosevelt acknowledged that the cryptanalytic efforts of military intelligence needed additional aid. Some Bletchley Park personnel went to America to train new code breakers, most of whom were members of the Women Accepted for Voluntary Emergency Service Corps (WAVES). WAVES assembled and trained to operate various bombes, eventually producing 121 bombes for used against seven different Japanese and German codes. After the Germans began sharing Enigma code secrets and teleprinter construction secrets with the Japanese in 1942, U.S. intelligence became more able to decipher

Japanese codes and could adapt Enigma bombe designs to fit Japanese Red and Purple codes.

**How a bombe worked: The mechanics of code breaking.** The Enigma teleprinter functioned by replacing plain text letters with random letters, chosen by the settings of a series of rotors individual to each letter and space in a plain text message. The Enigma machine had a possible 15 million, million ( $15 \times 10^{12}$ ) combinations, but within each rotor set, the combinations were far fewer. Repeated phrases, called “cribs,” such as common greetings or the name and ranks of officers, gave cryptographers a clue about the mathematical cycle of the rotors and how they replaced plain text letters. Once a series of these cycles was mathematically determined, the logic equation could be used to painstakingly decipher intercepts. The bombe worked on the concept that these cycles, and the equations representing them, could be replaced with electrical circuits.

The Turing Bombe replicated the rotors of a German Enigma machine, replacing the center reflecting rotor with a standard rotor that could be handset. The rotors were connected by a set of 26 parallel wires. The wire selected by the rotor positions determined the passage of voltage to the plug board. The machine then searched for various combinations of loops and live wires, assigning each a value on the plaintext/ cipher text rows of a diagonal board. A teleprinter decoded the messages on to synchronized paper tapes.

**Legacy of bombes.** By the end of the war, the bombe was still being used to decode enemy intercepts in the United States. British code breakers and engineers at Bletchley Park, however, invented a new machine, Colossus, that decoded messages more rapidly and with greater accuracy than the bombes. Colossus was the world’s first programmable computer, capable of decoding and transcribing messages without the cumbersome synchronization of paper tapes. The advent of punch-card computer processing ended the era of the code breaking bombe.

After the end of the war, British intelligence dismantled its operations as Bletchley Park. The numerous bombes, and Colossus, were disassembled or destroyed. The entire code breaking operation remained secret until the late-1980s, but after the news of Bletchley Park operations was broken to the public, historical preservationists sought to restore Bletchley Park and its code breaking apparatus. The British Computer Society’s Computer Conservation Society embarked on an ambitious endeavor to reconstruct Colossus and the Turing bombe in 1999.

#### ■ FURTHER READING:

##### BOOKS:

Hinsley, F. H. *British Intelligence in the Second World War*. Cambridge: Cambridge University Press, 1988.

Hinsley, F. H. and Alan Stripp, eds. *Codebreakers: The Inside Story of Bletchley Park*. Oxford: Oxford University Press, 2001.

Stinson, Douglas. *Cryptography: Theory and Practice*, second edition. Chapman and Hall, 2002.

#### SEE ALSO

*Codes and Ciphers*  
*Codes, Fast and Scalable Scientific Computation*  
*Colossus I*  
*FISH (German Geheimschreiber Cipher Machine)*  
*Operation Magic*  
*OSS (United States Office of Strategic Services)*  
*Poland, Intelligence and Security*  
*Purple Machine*  
*Ultra, Operation*  
*United Kingdom, Intelligence and Security*  
*World War II, United States Breaking of Japanese Naval Codes*

## Border Crossing and Inspection.

SEE *IBIS (Interagency Border Inspection System)*.

## Bosnia and Herzegovina, Intelligence and Security

Following World War I, the nations in the Balkan region were unified into a single state, known after 1929 as Yugoslavia. Tensions between the region’s ethnic populations remained high, but the establishment of a dictatorship under Marshal Tito kept Yugoslavia united after World War II. After Tito’s death, authoritarianism continued to dominate the Yugoslavian regime. The Yugoslavian intelligence community was dominated by secret police forces and government-backed political espionage. Modeled after intelligence and security forces in the Soviet Union, Yugoslav intelligence focused on protecting the ruling regime under the direct control of the Communist Central Committee.

In the early 1990s, Yugoslavia broke apart following the fall of the Soviet Union. In 1991 and 1992, the various ethnic states in the Balkan region declared their independence. Border disputes and ethnic tensions flared in the region, sparking intense warfare. The most intense conflict erupted in Bosnia and Herzegovina. The state was deeply divided. Bosniak Muslims, seeking autonomy, fought Serbian-backed forces. As the conflict escalated, the international community became concerned with the region’s endemic warfare. By the time United Nations and NATO forces intervened in the region, ethnic cleansing—genocide—plagued Bosnia and Herzegovina.

International intervention helped end genocide and warfare in the region, but civil war left the national infrastructure of Bosnia and Herzegovina devastated. In 1998, the Bosnian government began an ambitious program to rebuild the nation's intelligence and security forces. As of 2003, NATO-led Stabilization Forces (SFOR) continue to operate in Bosnia and Herzegovina, preserving peace in the region and aiding in the formation of new national security forces.

Bosnia and Herzegovina's main civilian intelligence service is the Agency for Investigation and Documentation (AID). The AID investigates current and past criminal activities, with a focus on ferreting out perpetrators of genocide and other war crimes. The investigative force also conducts domestic intelligence operations, including political and communications surveillance of military forces. The State Security Agency and the Civil Police work closely with the AID to assess and neutralize threats to national security, and protect the nation's citizens.

Although Bosnia and Herzegovina's military is greatly limited in their actions under the terms of current, regional cease-fire agreement, some military-based intelligence services continue to operate. The main objective of military intelligence services is to obtain foreign intelligence information, especially that which relates to the military strength of its neighboring states, Croatia and Serbia. Government-backed espionage against dissident and rival ethnic groups was circumscribed by international peacekeeping forces to deter renewed hostilities in the region.

The government also maintains a mixed civilian-military Anti-terrorist Brigade. Little is known about the daily operations of this secret police force.

#### ■ FURTHER READING:

##### ELECTRONIC:

Central Intelligence Agency. "Bosnia and Herzegovina" CIA World Factbook <<http://www.cia.gov/cia/publications/factbook/geos/bk.html>> (April 8, 2003).

##### SEE ALSO

*Croatia, Intelligence and Security*  
*Serbia, Intelligence and Security*  
*United Nations Security Council*

## Botulinum Toxin

■ BRIAN HOYLE

Botulinum toxin is among the most poisonous substances known. The toxin, which can be ingested or inhaled, and which disrupts transmission of nerve impulses to muscles, is naturally produced by the bacterium *Clostridium*

*botulinum*. Certain strains of *C. baratii* and *C. butyricum* can also be capable of producing the toxin.

Botulinum toxin has become well known in recent years for two reasons. First, the toxin has become a weapon in the arsenal of terrorists. Contamination of food is one route for infection with the toxin. The toxin can also be released into the air, which was attempted on at least three occasions between 1990 and 1995 by the Japanese cult Aum Shinrikyo. The government of Iraq admitted to United Nations inspectors following the 1991 Persian Gulf War that tens of thousands of liters of botulinum toxin had been produced and loaded into weapons. The toxin was the most numerous of all the biological weapons then developed by Iraq.

Paradoxically, the other reason for the toxin's fame is the use of the toxin as a cosmetic enhancement (i.e., "botox").

There are at least seven structurally different versions of botulinum toxin. The type designated as type A is responsible for some food-borne outbreaks in the United States and elsewhere. Improperly canned foods are a particular threat.

*Clostridium botulinum* is a spore-forming bacterium. Like the well-known anthrax bacillus, the spores of *Clostridium botulinum* can persist in the environment for many years and, when conditions become more favorable (i.e., in a wound, food, and the lungs) the spore can germinate and free the toxin. Dried preparations of the spores can thus represent a terrorist weapon.

The use of botulinum toxin as a weapon began in the 1930s, with experiments conducted by the Japanese on prisoners during the occupation of Manchuria. In World War II, plans were made to vaccinate Allied troops participating in the D-day invasion of Normandy, because of concerns that Germany had weaponized the toxin. Even the United States maintained an active biological weapons program, including the use of botulinum toxin, into the late 1960s.

Botulinum toxin acts by preventing the transmission of nerve signals between the nerves that connect with muscle cells. Progressive functional deterioration of the affected muscles occurs. Symptoms of botulinum intoxication include dizziness, blurred or double vision, nausea, vomiting, diarrhea, and weakness of muscles in various areas of the body. The muscle failure can be so severe as to lead to coma and respiratory arrest. Even in those who survive exposure to the toxin, complete recovery can take months.

#### ■ FURTHER READING:

##### BOOKS:

Tucker, J.B., (ed.). *Toxic Terror: Assessing the Terrorist Use of Chemical and Biological Weapons*. Cambridge: MIT Press, 2000.

## PERIODICALS:

- Byrne, M.P., and L.A. Smith. "Development of Vaccines for Prevention of Botulism." *Biochimie* no. 82 (2000): 955–966.
- Kahn, A.S., S. Morse, and S. Lillibridge. "Public-health Preparedness for Biological Terrorism in the USA." *Lancet* no. 356 (2000): 1179–1182.
- Montecucco, C. (ed.). "Clostridial Neurotoxins: The Molecular Pathogenesis of Tetanus and Botulism." *Current Topics in Microbiology and Immunology* no. 195 (1995): 1–278.
- Lacy, D.B., W. Tepp, A.C. Cohen, et al. "Crystal Structure of Botulinum Neurotoxin Type A and Implications for Toxicity." *Nature Structural Biology* no. 5 (1998): 898–902.

## ELECTRONIC:

- Centers for Disease Control and Prevention. "Botulism." Public Health Emergency Preparedness and Response. February 7, 2003. <<http://www.bt.cdc.gov/agent/botulism/index.asp>>(April 15, 2003).
- Johns Hopkins University. "Botulinum Toxin." Center for Civilian Biodefense Strategies. 2002. <<http://www.hopkins-biodefense.org/pages/agents/agentbotox.html>>(April 15, 2003).

## SEE ALSO

- Biological Warfare*  
*Microbiology: Applications to Espionage, Intelligence and Security*  
*USAMRIID (United States Army Medical Research Institute of Infectious Diseases)*

## Botulism.

SEE *Bioterrorism*.

---

## Brain-Machine Interfaces

---

■ JULI BERWALD

A brain-machine interface is the linkage of the brain to a mechanical device exterior to the body in such a manner that the device is controlled by natural signals from the brain. An important goal for developing such technology is to aid people who are paralyzed or otherwise physically impaired. The military has interest in brain-machine interfaces as a means of controlling robotics from a distance with extreme accuracy and precision.

One of the major technological hurdles in the development of brain-machine interfaces is the understanding of neural patterns required to accomplish tasks. One company headed by American scientist Phillip Kennedy has made great advances in this area. Kennedy has developed

a very small neurotropic device that is implanted into the motor cortex of the brain of severely paralyzed people. This device transmits electronic signals from the person's brain to electronic equipment that then translates the signals to a computer. People with the implant learn to control a mouse on the computer and to type text using electronic signals in their brain.

The extension of this technology is the understanding of the neural patterns required to control complex motor tasks. In 2000, scientists at Duke University implanted an array of 96 electrodes into the brain of an owl monkey. The electrical signals measured on each of the electrodes were collected when the monkey performed certain tasks, including reaching for food. These signals were then analyzed and mathematical algorithms were developed that allowed scientists to predict the trajectory of the monkey's hand from the neural signals. The scientists then programmed a robotic arm to move in three dimensions according to the monkey's brain signals. They eventually transmitted these signals over the Internet to a laboratory at MIT, where another robotic arm 600 miles away was controlled by the monkey's neural signals.

The Defense Advanced Research Projects Agency (DARPA) is extremely interested in brain-machine interfaces for controlling robotics and interpreting sensory information. In 2001, they authorized funding for the Brain-Machine Interfaces program. The goals of this program are to create new technologies that enhance human performance through non-invasive integration of neural signals into external devices. This includes understanding the neural codes required to complete complex motor tasks, building a feedback loop from an external device back to the brain, and fabricating new materials required to capture neural commands. In addition, biomimetic systems that integrate neural signals are of interest.

Other defense related projects investigate neural networks and optics. Scientists at the U.S. Army Aviation and Missile Command (Weapons Sciences Directorate) headquartered at the Redstone Arsenal, Alabama are working intently on projects designed to integrate optic "flow" and automatic target recognition systems. These projects utilize mathematical techniques improving image factorization (e.g., image decomposition). For example, neural network based optics using specific algorithms can translate optic flow into four separate image planes that represent various motion parameters. In addition to targeting, neural network based optics may be used to navigate autonomous vehicles and other robotics.

■ FURTHER READING:

## ELECTRONIC:

- Defense Advanced Research Projects Agency: Defense Sciences Office, "Brain Machine Interfaces" <<http://www.darpa.mil/dso/thrust/biosci/brainmi.htm>> (March 26, 2003).
- Neural Signals <<http://www.neuralsignals.com>> (March 26, 2003).

Science Daily: "Monkeys Control A Robot Arm Via Brain Signals" <<http://www.sciencedaily.com/releases/2000/11/001116080512.htm>> (November 16, 2000).

#### SEE ALSO

*Biological and Biomimetic Systems*  
*DARPA (Defense Advanced Research Projects Agency)*

---

## Brain Wave Scanners

---

The term *brain wave scanners*, in the context of law enforcement, encompasses an array of research studies and technological developments undertaken with the aim of using electronic equipment to determine the truth or falsity of an individual's statements. While such a concept may sound farfetched at first glance, it is based not on subjective phenomena, but on apparently measurable brain states. Using magnetic resonance imaging (MRI) and related equipment, it is possible to measure a subject's brain for increased activity that may indicate the telling of a lie.

The concept of a brain wave scanner is not unlike that of a polygraph, but whereas a polygraph measures fluctuations in heart rate and breathing, a scanner measures brain responses to stimuli. It could be more effective, because a "good liar" may experience little excitement in the circulatory system; however, even such an individual would be required to expend extra energy on the thought necessary to tell a lie, and it is this energy that a brain wave scanner may be able to measure.

It is often said that the truth is much easier to remember than a lie, and the activity measured by brain wave scanners offers a concrete illustration of this. When one is asked a question to which one knows the true answer, that answer comes first to mind automatically. Even if the individual has already prepared and rehearsed a lie, it is still necessary to think past the true answer and access the lie. This extra activity is easily measured on a brain scan.

### Testing and Possible Applications

In a 2001 University of Pennsylvania experiment using MRI, 18 subjects were given objects to hide in their pockets, then shown a series of pictures and asked to deny that the object depicted was in their pockets. Included was a picture of the object they had pocketed, meaning that the subject was lying when saying that the object was not in his or her pocket. At that juncture, the MRI recorded an increase of activity in the anterior cingulate, a portion of the brain associated with inhibition of responses and monitoring of errors, as well as the right superior frontal gyrus, which is involved in the process of paying attention to particular stimuli.

After the September 11, 2001, terrorist attacks, a number of government agencies began to take a new look at brain scanning technology as a means of security screening. In 2002, officials of the National Aeronautics and Space Administration reportedly informed airline officials that they were developing brain-monitoring technology for use in screening airline passengers. Such activity, along with an increase of interest in brain-wave scanning by the Federal Bureau of Investigation, has raised concerns among civil-liberties groups, which view brain-wave scanning as a particularly objectionable invasion of privacy in the service of public security.

#### ■ FURTHER READING:

##### PERIODICALS:

- Feder, Barnaby J. "Truth and Justice, By the Blip of a Brainwave." *New York Times*. (October 9, 2001): F3.
- Vedantam, Shankar. "The Polygraph Test Meets Its Match." *Washington Post*. (November 12, 2001): A2.
- Wright, Karen. "Go Ahead, Try to Lie." *Discover*. 22, no. 7 (July 2001): 21-22.
- Young, Emma. "Brain Scans Can Reveal Liars." *New Scientist*. (November 12, 2001).

#### SEE ALSO

*Brain-Machine Interfaces*  
*Electromagnetic Pulse*  
*Polygraphs*

---

## Brazil, Intelligence and Security

---

Brazil gained its independence from Portugal in 1822, seizing upon a period of European unrest to establish its own government. Since that time, the government of Brazil has been traditionally unstable, with large-scale landowners, the military, and democratic forces vying for political power.

A military coup took control of the nation for much of the late twentieth century, but civilians regained control of the government in 1985. Under military rule, political dissidents were taken into custody and sometimes tortured. The government used the intelligence services to conduct surveillance of citizens and infiltrate political organizations. The regime also imposed strict censorship. In 1989, Brazil had its first free elections in three decades. Seeking to distance the new government from the legacy of its predecessors, sweeping reforms were made to



demilitarize the national intelligence and security agencies. While Brazil's government has continued to weather scandal and presidential overthrow, the reformed intelligence community established in the early 1990s remains largely intact.

While the armed forces still maintain limited special intelligence units, most of Brazil's intelligence community is civilian. The Brazilian Intelligence Agency (ABIN) was created in 1995 to replace the Strategic Affairs Secretariat (SAE). The civilian government's first attempt at a reformed intelligence agency, the SAE supervised the Brazilian intelligence community from 1990–1994. Amid concerns that military interests dominated the agency, despite efforts to demilitarize its operations, the agency was dissolved and replaced with ABIN.

The Brazilian Intelligence agency is the main intelligence and security force in Brazil. Responsible for both internal and external intelligence, the agency coordinates operations between various operational branches and national law enforcement services. Charged with the protection of Brazilian interests both at home and abroad, ABIN collects and analyzes information from a variety of sources. The agency utilizes human, signals, and remote intelligence. The largest operational branch of ABIN is its counterintelligence unit. ABIN's counterintelligence division focuses on the protection of economic interests from sabotage, terrorism, and corporate espionage. The unit also conducts political surveillance of the military and coordinates efforts with law enforcement to ensure border security.

Today, Brazil has the sixth-largest population in the world. Its two largest cities, Sao Paulo and Rio de Janeiro, have respective populations of 19 and 10 million people. The most populous nation in South America, Brazil is one of the regions leading economies. In 2000, Brazilian intelligence began a series of operations targeting illegal business practices, including money laundering, trafficking of illegal drugs, and corporate espionage.

#### SEE ALSO

*Counter-Intelligence*  
*Economic Espionage*  
*Economic Intelligence*

## Brilliant Pebbles.

SEE *Strategic Defense Initiative and National Missile Defense*.

## British Secret Intelligence Service.

SEE *MI6 (British Secret Intelligence Service)*.

## British Security Service.

SEE *MI5 (British Security Service)*.

## British Terrorism Act

In July, 2000, the British Parliament passed the Terrorism Act, a lengthy piece of legislation that criminalized a number of activities associated with groups tied to terrorism. The act initially prescribed 14 groups, most of whom were involved in Northern Ireland's sectarian conflict. In March, 2001, Parliament passed an amendment to the act, listing 21 other organizations, of which most had a Middle Eastern base.

The British Terrorism Act is an example of the fact that, and while the United Kingdom and the United States have much in common politically, the British government reserves the right to exert far greater authority over freedom of speech than Washington. Whereas the Terrorism Act makes it illegal to possess certain written materials, in America, books on bomb-making and subversion are legal.

The Terrorism Act reformed or repealed earlier measures, including the Prevention of Terrorism Act of 1989, the Northern Ireland (Emergency Provisions) Act of 1996, and the Criminal Justice (Terrorism and Conspiracy) Act of 1998. It defined terrorism, listed proscribed organizations, established government powers against proscribed groups, provided for offenses relating to fund-raising for terrorists, gave the police authority to investigate terrorist groups, and criminalized a number of offenses, including the possession of information for terrorist purposes.

Within two weeks of the September, 2001 terrorist attacks in the United States, British authorities arrested four men under the British Terrorism Act. Among them was Sulayman Balal Zainulabidin, a 43-year-old cook. Another, Loifti Raissi, was wanted in Arizona on misdemeanor charges relating to his application for a pilot's license, but was thought to have been involved in training four of the terrorists involved in the September 11 attacks.

#### ■ FURTHER READING:

##### PERIODICALS:

Jackman, Tom. "Terror Suspect Allowed to Seek Foreign Aid." *Washington Post*. (July 18, 2002): B2.

Milbank, Dana, and T. R. Reid. "New Global Threat Revives Old Alliance." *Washington Post*. (October 16, 2001): A10.

##### ELECTRONIC:

London Man Charged Under British Terrorism Act. Cable News Network. <<http://www.cnn.com/2001/WORLD/europe/UK/10/04/inv.britain.arrest/>> (April 7, 2003).

Terrorism Act 2000. Her Majesty's Stationery Office. <<http://www.hmsso.gov.uk/acts/acts2000/20000011.htm>> (April 7, 2003).

#### SEE ALSO

*MI6 (British Secret Intelligence Service)  
Official Secrets Act, United Kingdom  
September 11 Terrorist Attacks on the United States  
United Kingdom, Counter-Terrorism Policy  
United Kingdom, Intelligence and Security*

## Brookhaven National Laboratory

■ K. LEE LERNER

Founded in 1947, Brookhaven National Laboratory is operated for the U.S. Department of Energy by Brookhaven Science Associates, a non-profit research company.

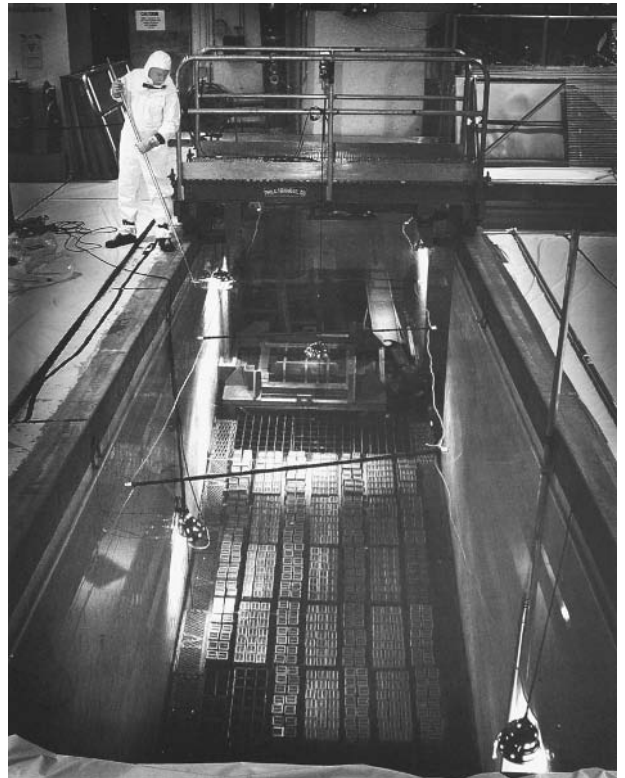
At Brookhaven, a staff of approximately 3,000 scientists, engineers, and technical support staff work alongside an additional 4,000 scientists and engineers who annually visit the facilities located on Long Island, New York.

Although research at Brookhaven impacts both basic science and national security related science issues, following the September 11, 2001, terrorist attacks on the United States, Brookhaven established an interdisciplinary working group to tackle specific issues related to counter-terrorism. The focus of the group is to oversee the development of technologies devoted to prediction, detection, and preemption, of terrorism.

An important component of Brookhaven projects is the development of sensors useful in detecting nuclear, chemical, and biological agents. For example, highly sensitive chemical sensors can detect explosives, and radiation detectors are useful in detecting contact with nuclear materials. Highly sensitive detectors are capable of measuring trace amounts in concentrations so small that the sensors can provide evidence of prior contact with suspect materials—even if the materials are no longer physically present.

Facilities at Brookhaven include a thermal neutron imaging camera that can detect radiation source emanation at distances up to approximately 200 feet. In addition, Brookhaven sensor systems utilize a number of physical properties—from laserscattering patterns to microwave probes—to interrogate unknown materials.

Biotechnology research at Brookhaven includes the development of vaccines to combat the deleterious effects of a broad spectrum of biological weapons and chemical



A Brookhaven National Laboratory employee works at a 68,000-gallon pool housing spent fuel rods in 1997, thought to be the source of a leak of radioactive materials that contaminated the groundwater source for Long Island's drinking water aquifer. AP/WIDE WORLD PHOTOS.

nerve gas agents. Antidote treatment research includes the development of topical creams that contain enzymes capable of degrading nerve agents.

To facilitate rescue of individuals in debris of collapsed buildings, Brookhaven engineers designed devices to help remove debris and to image debris fields. Magnetic imaging equipment can locate damaged structural elements (e.g., iron girders) and allow rescue personnel to evaluate structural integrity and identify possible areas of survival.

Brookhaven scientists and engineers developed the Mini-Raman Lidar System (MRLS) that is capable of detecting trace amounts of dangerous chemicals (including illegal narcotics and other drugs). Laser scattering devices can also detect distinct chemical profiles or "fingerprints." MRLS allows investigators to detect those chemical associated with the processing of nuclear fuels. Because MRLS is highly sensitive, inspectors can examine questionable objects from safer distances. In many cases, MRLS can accurately detect trace molecules at distances ranging from three to ten feet. Given the proper environmental controls, MRLS can detect trace molecules at far greater distances.

Another recent national security related project at Brookhaven National Laboratory involved the development

of the Large-Volume Radiation Detector that uses compressed xenon as part of a portable, battery powered, room-temperature spectrometer unit. The spectrometer is very sensitive and offers high discrimination and resolution at levels that allow investigators the ability to distinguish between isotopes used in medical products and those associated with prohibited nuclear activities. Investigators are hopeful that the success of the small scale detector will allow construction of larger units using similar technology that are capable of rapidly examining large cargo loads (e.g., bulk cargoes at truck terminals, ports, etc.) at safer “standoff” distances.

Other research facilities include a relativistic heavy ion collider, alternating gradient synchrotron, synchrotron light source, tandem Van de Graaff accelerators, high-field MRI, positron emission tomography (PET) facilities, transmission electron (TEM) and scanning (SEM) electron microscopes, a laser electron accelerator facility (LEAF), and other accelerator test facilities including 60-inch and 40-inch cyclotrons.

## ■ FURTHER READING:

### ELECTRONIC:

United States Department of Energy, Office of Science. National Laboratories and User Facilities. <[http://www.sc.doe.gov/Sub/Organization/Map/national\\_labs\\_and\\_userfacilities.htm](http://www.sc.doe.gov/Sub/Organization/Map/national_labs_and_userfacilities.htm)> (March 23, 2003).

United States Department of Homeland Security. Research & Technology. <<http://www.dhs.gov/dhspublic/display?theme=27&content=374>> (March 23, 2003).

Brookhaven National Laboratory. March 26, 2003. <<http://www.bnl.gov/world/>> (April 2, 2003).

### SEE ALSO

*Argonne National Laboratory*  
*DOE (United States Department of Energy)*  
*Environmental Measurements Laboratory*  
*Lawrence Berkeley National Laboratory*  
*Lawrence Livermore National Laboratory (LLNL)*  
*Los Alamos National Laboratory*  
*NNSA (United States National Nuclear Security Administration)*  
*Oak Ridge National Laboratory (ORNL)*  
*Pacific Northwest National Laboratory*  
*Plum Island Animal Disease Center*  
*Sandia National Laboratories*

---

## Bubonic Plague

---

### ■ BRIAN HOYLE

A concern of health and defense officials is the possible deliberate introduction of plague—or the exploitation of

plague—as a terrorist weapon. Plague causing microorganisms are highly lethal, highly transmissible, and relatively easy to develop as terrorist weapons.

Bubonic plague is transmitted via fleas infected with *Yersinia pestis*. Pneumonic plague results from plague bacterium invading lung tissue. Pneumonic plague exhibits an airborne form of transmission. Infection occurs from breathing aerosolized bacteria. Untreated pneumonic plague is highly lethal.

Bubonic plague is a disease that is typically passed from rodents to other animals and humans via the bite of a flea. The flea acquires the bacterium that causes the disease as it lives on the skin of the rodent. Humans can also acquire the disease by direct contact with infected tissue.

The bacterium *Pasteurella pestis* is also known as *Yersinia pestis*, after one of its co-discoverers, Alexandre Yersin.

Prior to 1970, both United States and Soviet biological weapons programs developed techniques that enabled weapons developers to aerosolize plague particles.

Bubonic plague is named because of the symptoms. The bacterial infection produces a painful swelling of the lymph nodes. These are called buboes. Often the first swelling is evident in the groin. During the Middle Ages, a pandemic of bubonic plague was referred to as the Black Death, because of the blackening of the skin due to the dried blood that accumulated under the skin’s surface.

The bubonic plague has been a significant cause of misery and death throughout recorded history. The Black Death is only one of many epidemics of plague that extended back to the beginning of recorded history. The first recorded outbreak of bubonic plague was in 542–543. This plague destroyed the attempts of the Roman emperor of the day to re-establish a Roman empire in Europe. This is only one example of how bubonic plague has changed the course of history.

The plague of London in 1665 killed over 17,000 people (almost twenty percent of the city’s population). This outbreak was quelled by a huge fire that destroyed most of the city.

The disease remains present to this day. In North America, the last large epidemic occurred in Los Angeles in 1925. With the advent of the antibiotic era, bubonic plague has been controlled in the developed world. However, sporadic cases (e.g., 10 to 15 cases each year) still occur in the western United States. In less developed countries (e.g., in Africa, Bolivia, Peru, Ecuador, Brazil) thousands of cases are reported each year.

The infrequency of bubonic plague outbreaks does not mean the disease disappears altogether. Rather, the disease normally exists in what is called an enzootic state. That is, a few individuals of a certain community (e.g., rodents) harbor the disease. Sometimes, however, environmental conditions cause the disease to spread through

the carrier population, causing loss of life. As the rodent populations dies, the fleas that live on them need to find other food sources. This is when the interaction with humans and non-rodent animals can occur. Between outbreaks, *Yersinia pestis* infects rodents without causing much illness. Thus, the rodents become a reservoir of the infection.

Symptoms of infection in humans begin within days after contamination with the plague bacterium. The bacteria enter the bloodstream and travel to various organs (e.g., kidney, liver, spleen, lungs) as well as to the brain. Symptoms include shivering, nausea with vomiting, headache, intolerance to light, and a whitish-appearing tongue. Buboes then appear, followed by rupture of blood vessels. The released blood can coagulate and turn black.

If the infection is untreated, the death rate in humans approaches 75%. Prompt treatment most often leads to full recovery and a life-long immunity from further infection. Prevention is possible, since a vaccine is available. Unfortunately, the vaccine is protective for only a few months. Use of the vaccine is usually reserved for those who will be at high risk for acquiring the bacterial infection (e.g., soldiers, travelers to an outbreak region). Antibiotics such as tetracycline or sulfonamide are used more commonly as a precaution for those who might be exposed to the bacterium. Such use of antibiotics should be stopped once the risk of infection is gone, to avoid the development of resistance in other bacteria resident in the body.

The most effective way to prevent bubonic plague is the maintenance of adequate sanitary conditions. This acts to control the rodent population, especially in urban centers.

In 1970, a World Health Organization study concluded that deliberate dissemination of 110 lbs (50 kg) of aerosolized *Y. pestis* over a city with a population of approximately 5 million people could potentially result in 150,000 cases of pneumonic plague. Half of these cases would require advanced medical care and approximately 20% would be expected to perish.

#### ■ FURTHER READING:

##### BOOKS:

- Campbell, G. L., and D. T. Dennis. "Plague and other *Yersinia* infections." In: D. L. Kasper, et al; eds. *Harrison's Principles of Internal Medicine*, 14th ed. New York: McGraw Hill, 1998.
- Dennis, D. T., N. Gratz, J. D. Poland, and E. Tikhomirov. *Plague Manual: Epidemiology, Distribution, Surveillance and Control*. Geneva: World Health Organization, 1999.
- Frist, W. H. *When Every Moment Counts: What You Need to Know about Bioterrorism from the Senates Only Doctor*. Lanham, MD: Rowman & Littlefield, 2002.
- Henderson, D.A., and T.V. Inglesby. *Bioterrorism: Guidelines for Medical and Public Health Management*. Chicago: American Medical Association, 2002.

Inglesby, Thomas V. "Bioterrorist Threats: What the Infectious Disease Community Should Know about Anthrax and Plague." *Emerging Infections* 5. Washington, D.C.: American Society for Microbiology Press, 2001.

##### PERIODICALS:

Kaufmann, A. F., M. I. Meltzer, and G. P. Schmid. "The Economic Impact of a Bioterrorist Attack: Are Prevention and Postattack Intervention Program Justifiable?" *Emerging Infectious Diseases* no. 3 (1997): 83–94.

##### SEE ALSO

*Antibiotics*  
*Biocontainment Laboratories*  
*Biological and Toxin Weapons Convention*  
*Biological Warfare*  
*Biological Weapons, Genetic Identification*  
*Bioterrorism, Protective Measures*  
*Chemical and Biological Defense Information Analysis Center (CBIAC)*  
*Chemical and Biological Detection Technologies*  
*Pathogen Transmission*  
*Pathogens*  
*Weapons of Mass Destruction*

## Bugs (Microphones) and Bug Detectors

■ BRIAN HOYLE

A key part of intelligence gathering and surveillance is the installation of listening devices. The classic Cold War image of Soviet espionage agents secretly planting "bugs" in an office of the United States embassy is an accurate historical picture of the use of these listening devices. Police forces and private investigators also use bugging devices (with legal approval).

The use of listening devices is often a race to acquire information before the devices are discovered and removed. For example, rooms where top-secret intelligence activity occurs are frequently examined, or "swept", for bugs.

A typical electronic bug consists of a microphone and a radio transmitter. The microphone receives sound waves and either vibrates a thin membrane called a diaphragm (a dynamic microphone) or a thin metal ribbon suspended in a magnetic field (a ribbon microphone). Vibration of the diaphragm produces an electrical signal. Vibration of the metal ribbon produces a voltage change, which can be converted to an electrical signal.

The electric signals are then beamed out of the transmitter portion of the bug to a receiver. The conversation



Sinn Féin President Gerry Adams displays an electronic tracking and listening device, found in a car used by Sinn Féin leaders, during a press conference in Belfast, Northern Ireland in 1999. AP/WIDE WORLD PHOTOS.

transmitted by the bug to the receiver can be recorded or listened to directly. Other types of bugs exist. For example, radio frequencies passing through the electrical wiring of a building can be intercepted. Bugs can also intercept the electrical transmissions from portable phones, wireless computers linked to a network, and even from a computer monitor.

The designation of secret listening devices as bugs is entirely suitable, given their small size. Modern bugs can be concealed in pens, calculators, and even buttons (although the latter need to be replaced frequently, as their power supply is so small).

The miniaturization of electronics has made it possible to pack more devices into the small package. For example, video equipment can be contained in a bug, enabling sight as well as sound surveillance.

Up to the 1980s, bugs operated using very high frequency, or VHF, radio waves. However, the development of mobile communications technology, particularly digital

telephones, paved the way for the development of bugs that operate using ultrahigh frequency wavelength or microwaves. This has made the detection of bugs more difficult than simply detecting the output of radio waves. Some modern bugging devices can also disguise the output signal or vary the frequency of the signal, which can thwart detection.

Some bugs contain voice-activated recorders that are capable of storing up to 12 hours of conversation. The information can then be rapidly sent to a receiver in a “burst” transmission. Because detection of the bug is geared toward the frequencies emitted during transmission, the detection of these bugs is difficult. Counter systems are designed to try and activate the bug and then detect it. The transmission range of bugs has improved from mere yards to miles. Some bugs can even transmit to satellites, making monitoring from thousands of miles away feasible.

Another surveillance option is the use of a microphone. Conventional microphones operate electronically; the electrical signals representing the converted sound waves are passed through a wire to a receiving device located elsewhere. Microphones that operate using magnetic fields also exist.

Shotgun microphones equipped with a parabolic reflector can record conversation outside at a distance. Electronic filters screen out extraneous background noise in order to enhance the sensitivity of the microphone.

Laser microphones bounce a laser beam off of an object that is near the conversation. The object must be something that resonates, or is able to move as pressure waves created by noise in the room encounter it. As the object vibrates back and forth due to the sound waves from the conversation in the room, the distance traveled by the laser beam will become slightly shorter and longer. These length differences can be measured over time, and the pattern of the vibrations translated into the text of the conversation.

Microphones are extremely hard to detect, especially when used in a room where other electrical appliances (i.e., computers, telephones) are operating.

Bugs are detected by virtue of the frequencies they emit. Essentially a bug detector is a receiver. When brought near an operating bug, the detector will collect and amplify the bug’s transmission. Bug detectors are now portable enough to be carried in a “sweep” of a room.

Bugs and microphones have moved from the arena of political espionage to the boardrooms of corporate offices and police surveillance operations. Recognizing the prevalence of electronic eavesdropping devices and their threat to privacy, the United States Congress passed the Electronic Communication Privacy Act in 1986, which made bugging illegal. Nonetheless, the use of eavesdropping devices and detectors is widespread in the intelligence

and business communities. One estimate places the annual sales of such devices in the United States alone at \$888 million.

#### ■ FURTHER READING:

##### BOOKS:

Shannon, Michel L. *Bug Book: Everything You Ever Wanted To Know About Electronic Eavesdropping...But Were Afraid To Ask*. Boulder, CO: Paladin Press, 2000.

Shannon, Michel L. *Don't Bug Me: The Latest High-Tech Spy Methods*. Boulder, CO: Paladin Press, 2002.

##### SEE ALSO

*Codes and Ciphers*  
*Computer Hackers*  
*Internet Surveillance*

#### Burn Box.

SEE *Document Destruction*.

---

## Bush Administration (1989–1993), United States National Security Policy

---

■ CARYN E. NEUMANN

The administration of President George H. W. Bush confronted the most fundamental changes in the national security environment since the onset of the Cold War in the 1940s. The collapse of the Soviet Union and the disintegration of the Soviet empire removed the threat of communism that had long determined the direction of security efforts. To respond to this changed environment, Bush reduced the size of the military, shifted resources to the war on drugs, and pursued a new world order that included access to the oil-rich Persian Gulf states. This last goal made imperative the removal of Iraqi forces from Kuwait after it was invaded by Iraq, and resulted in the U.S. coalition-led Persian Gulf War with Iraq.

Bush, a former director of the Central Intelligence Agency, entered the White House after serving as vice president to Ronald Reagan. His approval of Reagan's security policies meant that he would largely continue them as president. The appointment of General Brent Scowcroft, National Security Adviser during the Ford administration, brought deep experience to the National

Security Council (NSC) leadership. James Baker headed the State Department. The Department of State and the NSC worked harmoniously, with the jealous guarding of territory that had marked earlier administrations notably absent from this administration.

Reagan had issued a 1986 directive that characterized illegal drugs as a national security threat. The Bush administration expanded this initiative in 1989 with National Security Directive (NSD) 18. This two-part NSD designated the Department of Defense as the lead agency for the detection and monitoring of the aerial and maritime transit of illegal drugs into the country. While there are few specifics in the document, implementation of the directive almost certainly included increased use of intelligence resources, specifically more extensive use of U.S. reconnaissance satellites to locate coca-growing laboratories, communication intercepts to identify drug-smuggling planes entering the country, and other efforts to help monitor the communications of major drug cartel leaders. The second part of the NSD, named the "Andean Initiative", called for foreign aid for Columbia, Bolivia, and Peru with most of the assistance coming in the form of military equipment, such as helicopters, patrol boats and ammunition. The NSD also included such intelligence aid as radars, electronic sensors, secure communications equipment, and computers to store and retrieve information about drug traffickers.

Along with freeing resources for the war on drugs, the end of the Cold War also brought a renewed emphasis on arms control. The collapse of the Soviet system had left a considerable amount of military hardware in Europe and Bush saw arms control as a way of reducing the risks associated with this weaponry. The Conventional Forces Europe (CFE) agreement in 1990 covered the area from the Atlantic Ocean to the Urals. The North Atlantic Treaty Organization (NATO) forces and the recently Soviet-aligned divisions of the Warsaw Treaty Organization (WTO) were limited to 20,000 tanks; 30,000 armored combat vehicles; 20,000 artillery pieces; 2,000 helicopters; and 6,800 combat aircraft. These figures meant marginal cuts for NATO countries, but substantial cuts for WTO states. The result was parity in conventional military forces. CFE served as a major symbol of the end of the Cold War by speeding the demilitarization of Europe.

The dependency of the United States upon oil made access to the Persian Gulf a vital matter of national security. In NSD 26, Bush ordered federal agencies to expand political and economic ties with the Saddam Hussein regime of Iraq to ensure the continued friendliness of the dictator. This 1989 directive led to U.S. government loan guarantees that enabled Iraq to purchase vital foodstuffs on credit and divert hard currency reserves to finance a massive arms buildup. In 1990, Iraq used these arms to support an invasion of Kuwait. The resulting Persian Gulf War succeeded in freeing Kuwait from Iraq's grasp, but U.S. national security interests were damaged in the long term by allowing Hussein to remain in power.

■ FURTHER READING:

BOOKS:

Williams, Phil and Dilys M. Hill, eds. *The Bush Presidency: Triumphs and Adversities*. New York: St. Martin's Press, 1994.

ELECTRONIC:

Digital National Security Archive. "Presidential Directives on National Security from Truman to Clinton." <<http://nsarchive.chadwyck.com/pdessayx.htm>> (April 25, 2003).

SEE ALSO

*Cold War (1972–1989): The Collapse of the Soviet Union*  
*National Security Strategy, United States*  
*NATO (North Atlantic Treaty Organization)*  
*NSC (National Security Council)*  
*Persian Gulf War*

---

## Bush Administration (2001–), United States National Security Policy

---

■ CARYN E. NEUMANN

George W. Bush, transformed the national security system of the United States to combat the threat of global terrorism. After the terrorist attacks of September 11, 2001, Bush faced the likelihood of a repeat attack with the knowledge that terrorism could not be effectively addressed through traditional defensive strategies. Accordingly, the administration developed a homeland security



Former U.S. CIA Director Robert Gates, left, visits with former Russian President Boris Yeltsin, second from left, at the Kremlin during the first trip to Moscow by the head of the U.S. intelligence agency in 1992. Also shown are Victor Barannikov, right, former Minister of Security, and Yvgeny Primakov, second from right, former head of the Russian Foreign Intelligence Service, the successor to the KGB. AP/WIDE WORLD PHOTOS.



President Bush meets with his National Security Council in the White House situation room in October, 2001. Clockwise, from center are: White House Chief of Staff Andrew Card, Vice president Dick Cheney, President Bush, Secretary of State Colin Powell, Defense Secretary Donald Rumsfeld, and National Security Advisor Condoleezza Rice. AP/WIDE WORLD PHOTOS.

system and advanced a new doctrine that took into account the shadowy nature of terrorism. With this theory of pre-emption, Bush argued that the U.S. possessed the right and the moral responsibility to launch preventive strikes against states that posed a danger to national security even when that danger was not imminent. This doctrine led to the U.S. led attack upon Iraq, Operation Iraqi Freedom, in 2003.

Bush, a past governor of Texas, took office with little experience in foreign affairs. Nine months into his presidency, the terrorist attacks of September 11, 2001, revealed shortcomings in national security. Simply, the major institutions of American national security were designed during the Cold War to meet the requirements of that era and failed to adequately protect the U.S. from the twenty-first century threat of global terrorism. To meet the challenge of retooling the security system, Bush relied upon Donald Rumsfeld as Secretary of Defense, Colin Powell as Secretary of State, and Condoleezza Rice as National Security Advisor.

In order to address terrorism, the Bush administration changed the way that security threats were identified and monitored. Designed with the aim of collecting information about the massive and immobile Soviet bloc, the

intelligence community now had to follow a far more complex and elusive set of targets. The administration strengthened intelligence warning and analysis to provide integrated threat assessments for national and homeland security. Through such new creations as the Terrorist Threat Integration Center and the use of such older networks as Interpol, the U.S. disrupted terrorist networks, removed key leaders, and arrested more than 3,000 terrorists around the world. The new Department of Homeland Security intensified security at borders and ports of entry through measures that included posting more than 50,000 federal screeners in airports.

Afghanistan had provided a safe base for al-Qaeda terrorists to plot against the U.S. and this country became the first target of an anti-terrorism strike. The 2001 war in Afghanistan aimed to capture al-Qaeda leader Osama bin Laden, remove a government that had permitted the growth of terrorism, and establish a democratic system. While the government quickly collapsed and the terrorist support network appears to be shattered, bin Laden, as of June, 2003, has not been captured. Significant numbers of U.S. military forces remain in the country to continue the search for terrorists and to serve as peacekeepers.



In the months after the Afghanistan attack, the Bush administration honed a doctrine of pre-emption that justified military aggression as the prevention of evil-doing. Bush sought to persuade other nations to adopt this doctrine as part of an effort to protect the U.S. and its allies from attack by strengthening alliances to defeat global terrorism. The refusal of many other countries to cooperate for reasons that included nationalism and anger at perceived American arrogance has meant that some of these alliances have not formed. The 2003 war upon Iraq became an Anglo-American project to prevent Saddam Hussein from employing weapons of mass destruction and supporting terrorism.

Under Bush, the United States possesses the strongest military that the world has ever known. The global arms race is over, with no nation able to match the U.S. in naval, air, missile, or tank strength and only China offering a larger ground force. The ability of a large military to ensure national security, however, is not certain. The historic hostility of Arabs to Western intervention may

complicate efforts to stabilize the Middle East and establish a model of democracy in Iraq and Afghanistan. With the perspective of history, therefore, the accomplishments of the Bush administration can be fully evaluated.

■ FURTHER READING:

ELECTRONIC:

White House. "National Security." <<http://www.whitehouse.gov/response/index.html>> (April 27, 2003).

SEE ALSO

- Domestic Intelligence*
- Enduring Freedom, Operation*
- Homeland Security, United States Department*
- Interpol (International Criminal Police Organization)*
- Iraq War: Prelude to War (The International Debate Over the Use and Effectiveness of Weapons Inspections.)*
- Iraqi Freedom, Operation (2003 War Against Iraq)*
- Terrorist Threat Integration Center*
- United States, Counter-terrorism Policy*
- World Trade Center, 2001 Terrorist Attack*



## Cambodian Freedom Fighters (CFF)

Cambodian Freedom Fighters (CFF) also operates as, or is known as, the Cholana Kangtoap Serei Cheat Kampouchea.

CFF emerged in November, 1998, in the wake of political violence that saw many influential Cambodian leaders flee and the Cambodian People's Party assume power. With an avowed aim of overthrowing the government, the group is led by a Cambodian-American, a former member of the opposition Sam Rainsy Party, and its membership includes Cambodian-Americans based in Thailand and the United States and former soldiers from the separatist Khmer Rouge, Royal Cambodian Armed Forces, and various political factions. The CFF has on at least one occasion attacked government facilities and planned other bombing attacks. In late November, 2000, the CFF staged an attack on several government installations, during which at least eight persons died and more than a dozen were wounded, including civilians. The group's leaders claimed responsibility for the attack. Following a trial of 32 CFF members arrested for the attack, five received life sentences, 25 received lesser jail terms, and two were acquitted. In April, 1999, five other members of the CFF were arrested for plotting to blow up a fuel depot outside Phnom Penh with antitank weapons.

CFF's exact strength is unknown, but totals probably never has exceeded 100 armed fighters. CFF operates in Northeastern Cambodia near the Thai border. Its U.S. based leadership collects funds from the Cambodian-American community.

### ■ FURTHER READING:

#### ELECTRONIC:

CDI (Center for Defense Information), Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <<http://www.cdi.org/terrorism/terrorist.cfm>> (April 17, 2003).

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001," Annual Report: On the Record Briefing. May 21, 2002 <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual Reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

#### SEE ALSO

*Terrorism, Philosophical and Ideological Origins  
Terrorist and Para-State Organizations  
Terrorist Organization List, United States  
Terrorist Organizations, Freezing of Assets*

## Cambridge University Spy Ring

### ■ ADRIENNE WILMOTH LERNER

The Cambridge spy ring was a group of British young men recruited as Soviet spies in the 1930s. The group was known in Britain as the Cambridge spy ring, after the University where the men attended classes and were recruited for espionage. In the Soviet Union, the group was known as the "magnificent five." The Cambridge spy ring infiltrated the highest level of the British government, including MI-5, MI-6, the Foreign Office, and the War Ministry. During their career, the group betrayed some of



Kim Philby (right) shown here following the shelling of his vehicle during the Spanish Civil War, was a member of the Communist Party while at Cambridge University, where he recruited and led a ring of spies for the Soviet Union. ©BETTMANN/CORBIS.

Britain's most guarded secrets to the Soviet Union. The group was led by master-spy, Harold "Kim" Philby.

Soviet agents planned to expand their espionage network in Britain as early as 1928. Though several spies operated successfully in Britain at the time the Cambridge ring was founded, Soviet intelligence officials realized that it was necessary to recruit people who had access to the upper echelons of British society, who could land prestigious civil service jobs, to infiltrate the highest levels of British government. To that end, Soviet agents began recruiting young men at Oxford University and Cambridge University into service. They looked for students who held genuine communist or socialist political sympathies, and who possessed the necessary social pedigree to obtain the confidence of high level peers. From Cambridge, Soviet agents persuaded Kim Philby, Guy Burgess, Donald Maclean, Anthony Blunt, and John Carincross into service for the Soviet Union.

**Kim Philby.** After graduating Cambridge, Kim Philby (1912–1988) failed to land a position in the Foreign Service. He worked briefly at the *London Times*. Philby proved

his worth to Soviet intelligence during this time by smuggling agents and communist supporters out of fascist Austria. He then traveled to Spain as a war correspondent, covering the Spanish Civil War. When World War II began, Philby returned to Britain, finally securing a job with British Intelligence.

From 1944 to 1946, Philby served as director of anti-Soviet counterintelligence for British Intelligence. The position guaranteed his access to top-level British military, intelligence, and government secrets, including World War II battle plans and Cold War agreements between Britain and the United States to thwart the spread of communism in Europe.

In 1949, Philby was stationed in Washington, D.C. as part of an Anglo-American intelligence cooperative operation. For three years, Philby had access to CIA and FBI files. More damaging, he received briefings of Venona Project intercepts, providing him with the ability to inform Moscow of United States efforts to break Soviet communications codes. The Venona intercepts also allowed Philby to monitor American knowledge of Soviet spy networks within

the United States, and report defections to Soviet authorities. After returning to London in 1951, Philby continued his career as a mole (double agent) for over a decade.

**Guy Burgess.** Guy Burgess (1910–1963) worked as a radio correspondent for the BBC from 1936 through 1944. During World War II, Burgess was also employed by British intelligence agency, MI5. Burgess was somewhat successful in transmitting messages to Soviet agents via radio broadcasts and smuggled several key documents to Moscow. Burgess stole some of the most sensitive information in the career of the Cambridge spy ring. While working for MI-5 in London, he smuggled copies of documents relating to nuclear weapons development. He also informed the Soviet government of United States and British plans to create the North Atlantic Treaty Organization (NATO), a European-American military alliance system.

In 1950, Kim Philby requested that Burgess be assigned to the Washington, D.C., bureau of the British Foreign Office. Burgess worked as Philby's assistant until he came under the suspicion of British intelligence. Philby then sent Burgess back to London, presumably to avoid suspicion upon himself.

**Donald Maclean.** The third member of the Cambridge spy ring, Donald Maclean (1913–1983), worked closely with Burgess. After graduating from Cambridge, Maclean worked in diplomatic service. In 1950, he became head of the Foreign Office's American Department.

While working at the British Embassy in Washington, D.C., Maclean was the main source of information regarding United States and British communications, advising Moscow on Anglo-American policy. In 1951, Maclean was tapped to be the British representative on the American-British-Canadian council on the sharing of atomic secrets. With Burgess, Maclean used his position to funnel highly classified atomic secrets to Soviet military intelligence. The two men did not steal technical information about the atomic bomb, but did provide Moscow with accurate assessments of the American atomic arsenal, production capabilities, and nuclear resources.

**The Defections of Maclean, Burgess, and Philby.** In 1949, Robert Lamphere, an FBI counterintelligence agent working with the Venona project, discovered that someone was sending telegraph messages from the British Embassy in Washington, D.C. to Moscow. The sender, under the codename "Homer" was later identified as Maclean. Philby, while working in Washington, learned of the FBI investigation of Maclean. Philby then devised a plan to warn Maclean of his impending exposure, while protecting himself and the rest the Cambridge spies.

Philby and Burgess agreed that Burgess would endeavor to be recalled by the Foreign Office to London, where he could arrange to meet with, and warn Maclean without arousing suspicion. Since Burgess had lived in the

Philby family home while assigned to his Washington, D.C. post, Philby cautioned Burgess not to attempt to defect to the Soviet Union with Maclean should he decide to escape. Burgess agreed to escort Maclean to safety, but to return to Britain to avoid drawing attention to other members of the Cambridge ring.

Days before he was scheduled to be questioned by British and American intelligence officials, Maclean, with Burgess, escaped to France. Once on the continent, they made their way to Moscow via a network of KGB safe houses. Soviet authorities insisted that Burgess defect with Maclean. Burgess lived in Russia until his death in 1963, though he reportedly did not attempt to further participate in the Soviet government. Maclean learned Russian and spent his remaining years working as an economic analyst and advisor on Western policy.

When British intelligence learned of Burgess and Maclean's defection, and acknowledged their roles in Soviet espionage operations, Philby was immediately placed under suspicion as a possible Soviet mole. In 1955, he deftly weathered MI-5 and MI-6 interrogation. After being released from his job at MI-6, he later was permitted to return to the civil service. Philby continued to act as a mole for Soviet intelligence for several more years, though he had limited access to top-secret materials.

In 1963, under renewed suspicion of espionage, Philby took a position as Foreign Office correspondent in Beirut, Lebanon. Later that year, a Soviet intelligence agent defected to the West. While being interrogated by Australian and British intelligence in Sydney, the defector named Philby as one of the Soviet's greatest human intelligence assets. Philby quickly defected to the Soviet Union, where he spent the rest of his life. He worked with the KGB, training spies for operation in the West. Cambridge spy ring member Anthony Blunt aided Philby's final escape.

**Anthony Blunt.** Though not the most active spy in the Cambridge ring, Anthony Blunt (1907–1983) aided Soviet agents' recruitment efforts at Cambridge. Blunt supplied the names of possible moles, and regularly attended communist political meetings in search of young recruits.

Blunt received degrees in history and art history from Cambridge. At the outbreak of World War II, Blunt went to work for British Intelligence. Blunt lacked the high-level security clearances possessed by other Cambridge spy ring members, however he was successful in smuggling photographs of documents regarding British troop locations and counterintelligence reports to his KGB contact, Yuri Modin. Blunt also provided information to Soviet military intelligence regarding British code breaking efforts against the Germans. After the war, he cultivated a reputation as a leading national academic. Socially, he often refused to comment on national and international political matters, leading colleagues to believe he had grown disillusioned and possessed little interest in the subject.

Though Blunt did conduct espionage for the Soviets after World War II, a majority of his operations was conducted during wartime. He was the first member of the Cambridge spy ring to retire from service, returning to his career as an art historian and museum curator, and the only member to remain in Britain.

In 1964, an American, Michael Straight, who had attended Cambridge with Blunt told FBI and MI-5 agents that Blunt had tried to recruit him to spy for the Soviet Union. After being exposed as a member of the Cambridge spy ring, Blunt provided MI-5 and MI-6 with some information regarding his past operations and associates, most of whom had by 1964 died or defected to Russia and were out of reach of British prosecutors. In exchange, Blunt was not tried for his offenses. He continued his career in art history, managing the Courtauld Collection until his retirement. His career as a spy for the Soviet Union was exposed to the public by the government officials under Prime Minister Margaret Thatcher in 1979. He was stripped of his knighthood and academic honors. By the time of his exposure, the public was already well acquainted with the stories of agents Maclean, Burgess, and Philby. Blunt was then presumed to be the final member of the infamous Cambridge spy ring.

**John Carincross.** In 1990, a fifth member of the Cambridge ring was publicly identified. John Carincross (1913–1995) worked with Maclean in the Foreign Office before being transferred to the offices of the Treasury in 1940. Through his connections with British intelligence and the Treasury, Carincross obtained a significant amount of information about the British Cipher School and code-breaking program at Bletchley Park. Heeding Carincross's warnings, Soviet intelligence changed their diplomatic, military, and intelligence codes before the end of World War II. Bletchley Park cryptologists thus, had to begin anew with efforts to break the Soviet code.

Carincross also leaked information about British and American nuclear programs. Analysts estimate that the Soviet Union was able to develop nuclear weapons three years faster, and millions of dollars cheaper, with the aid of intelligence from moles such as the Cambridge spies.

Similar to Blunt, when Carincross was exposed, he provided information about Soviet espionage networks to British intelligence. While the ultimate usefulness of such information remains the subject of debate, he was nonetheless granted some level of immunity from prosecution. When his career as a Soviet spy was made public, he left England for France.

**The legacy of the Cambridge University spy ring.** The actual damage to British and American national security caused by the activities of the Cambridge spy ring may never be fully assessed. Even with the declassification of reports and archives in the former Soviet Union, a comprehensive account of secrets stolen by the ring remains illusive. The

Cambridge spies did have a profound short-term influence on British and American intelligence operations. Both nations stepped up counterespionage efforts to root out similar moles in government agencies. Competitive tensions between MI-5 and MI-6 in Britain, and the CIA and FBI in the United States, were greatly exacerbated after Kim Philby's defection. The agencies blamed each other for not conducting adequate background checks on British personnel sent to work on joint Anglo-American intelligence operations, and for not discovering the Soviet spy network in time to prevent the loss of substantial information. The incident humbled both the British and American intelligence communities, and even fostered mistrust between the two nations. For a decade, Britain and American intelligence forces shared only limited information.

Relations between the British and American intelligence communities gradually became more supportive, eventually returning to the cooperative status enjoyed in the early Cold War years. When the Cold War ended with the fall of the Soviet Union, the extent to which rival nations infiltrated each other's governments with spy networks was made apparent. Declassification of documents relating to Cold War espionage proved the Cambridge spy ring was far from alone in its operations.

The Cambridge ring gained its notoriety not only from its exploits of espionage, but also because of its seemingly unlikely cast of characters—upper class, well-schooled, British citizens who fit well into the “old boys” network that dominated the British civil service. Their social credibility helped them gain access to the nation's top secrets. Further complicating the legacy of the spy ring was the effectiveness with which the group operated. Philby, Burgess, Blunt, Maclean, and Carincross spent years building reputations as loyal British citizens and staunch anti-communists before beginning active espionage during World War II. With the exception of one payment made to Kim Philby when his family was in dire financial need, none of the Cambridge spies demanded compensation for their services to Soviet intelligence. The group thus seemed ideologically loyal to communism, as opposed to performing espionage for personal gain.

Regardless of motive or the ultimate success of their operations, the Cambridge spies are some of the most infamous figures of British intelligence. Subsequent incidences of British citizens in the employ of Soviet intelligence stealing sensitive information from high-level officials further embarrassed British intelligence. In 1963, the Profumo Affair exploded to public attention when intelligence agents and journalists learned that the mistress of a British cabinet minister was a Soviet informant. The “Sex for Secrets” scandal helped bring down the administration of Prime Minister Harold Macmillan. Ironically, Macmillan, while serving as Foreign Secretary, cleared Kim Philby of wrong-doing eight years before his ultimate defection.

Labeled traitors in Britain and America, the “magnificent five” enjoyed fame in the Soviet Union. When Kim

Philby died there in 1988, he was buried in Moscow with full state honors.

#### ■ FURTHER READING:

##### BOOKS:

Boyle, Andrew. *The Climate of Treason: Five Who Spied for Russia*. London: Hutchinson, 1979.

Brown, Anthony Cave. *Treason in the Blood*. Boston: Houghton Mifflin, 1994.

##### PERIODICALS:

Teagarden, Ernest M. "The Cambridge Five: The End of the Cold War Brings Forth Some Views from the Other Side." *American Intelligence Journal* 18, no. 1/2 (1998): 63–68.

##### SEE ALSO

*Cold War (1945–1950), The Start of the Atomic Age*

*Cold War (1950–1972)*

KGB (Komitet Gosudarstvennoi Bezopasnosti, *USSR Committee of State Security*)

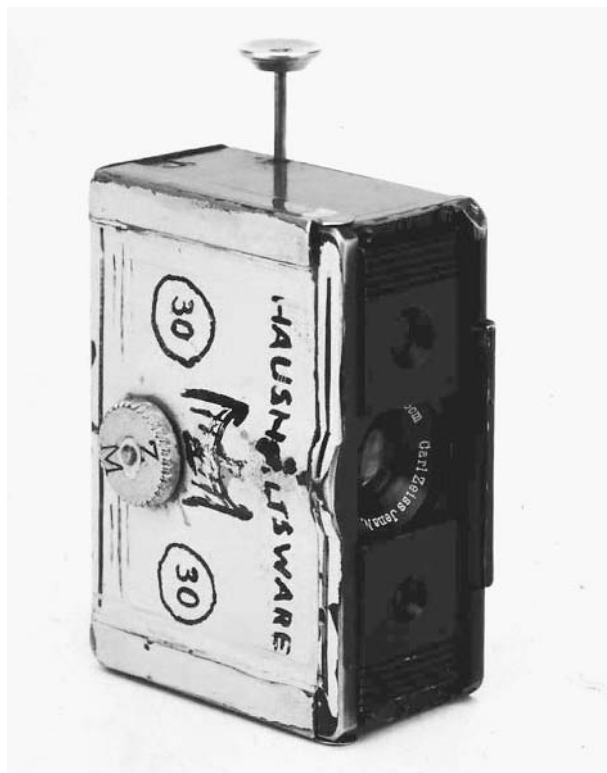
MI5 (*British Security Service*)

MI6 (*British Secret Intelligence Service*)

OSS (*United States Office of Strategic Services*)

*Soviet Union (USSR), Intelligence and Security*

*Special Relationship: Technology Sharing Between the Intelligence Agencies of the United States and United Kingdom*



A circa 1938 top secret spy camera made to resemble a contemporary German matchbox. AP/WIDE WORLD PHOTOS.

## Cameras

#### ■ JUDSON KNIGHT

Cameras have a number of applications in the world of security and espionage. Cameras can be used for conducting surveillance, for instance, an activity that may require neither proximity to the subject nor even a human operator. More intriguing and wide-ranging, however, are the uses of the camera in up-close work by intelligence operatives. Such situations require human ingenuity, not only for designing effective photographic equipment, but also for concealing the camera and its operations. Intelligence personnel have used cameras to photograph individuals and their activities, as well as buildings and installations. A significant subcategory of espionage photography involves the copying of documents, often with special cameras, although sometimes with ordinary equipment.

### Background

A camera functions by focusing light through a lens onto a surface coated with light-sensitive chemicals. The concept of the camera dates back to the Renaissance idea of

the camera obscura, a small, dark chamber into which light was permitted only through pinholes. During the early nineteenth century, inventors perfected the camera obscura to make the prototype of the modern camera, but early photography was a cumbersome affair characterized by large, boxy cameras and slow exposures. It is for this reason that most photographs from the American Civil War—the first conflict chronicled in depth by photojournalists—tend to be stills rather than action shots.

Only in the twentieth century was it possible to build cameras useful for work in espionage. Particularly after World War II, the number of possible camera types suited either to speed, concealment, range, or photographic resolution proliferated along with the many uses to which espionage and security organizations applied them. Today, the principal uses for cameras in the security and espionage context are copying documents, capturing activities of individuals at a close range, or conducting surveillance on large groups over large areas from a distance.

The last of these activities, while certainly a significant part of espionage and security operations, typically lacks the tactile qualities popularly associated with the use of cameras by spies. Surveillance aircraft such as the U-2 and SR-71 Blackbird, as well as satellites of the KH or “keyhole” series, carried sophisticated cameras for long-range photography of missile installations, weapons factories, and other facilities. In such a situation, the human

operator of the camera plays a lesser role than the technology behind its operation, and that of the craft that keeps it aloft many thousands of feet or miles above Earth's surface.

**Surveillance cameras in daily life.** Similarly, with close-range surveillance and security cameras that operate automatically, the human operator is of little significance. Still, there is a great deal of immediacy and intimate contact between camera and subject—especially because the unwitting subject seldom knows the degree to which he or she is under surveillance. In modern times, Americans have become accustomed to ordinary security cameras in stores and other businesses, particularly those whose contents have high monetary value. According to the Security Industry Association, by 2003, there were some two-million closed-circuit television systems in operation, most of them operated by private businesses for security purposes, in the United States. CCS International, a security company, estimated that the average person in Manhattan was photographed 73 to 75 times a day. Often this happened when the individual was not aware of the surveillance, even when the camera itself was in plain view. That camera might well be a dummy, with the real camera photographing an individual's activities from another angle.

Although civil libertarians protested this proliferation of security cameras, they are unlikely to disappear any time soon. J. P. Freeman, a firm that performs marketing research for the security industry, estimated in 2002 that the market for digital video surveillance equipment was growing at the rate of fifteen percent per year, particularly noticeable gains during the early twenty-first century recession. Additionally, in the heightened climate of awareness that followed the terrorist attacks of September 11, 2001, Americans were less likely than ever to react to potential violations of privacy.

**In communist Eastern Europe.** If surveillance cameras are ubiquitous in a democratic nation such as the United States, they are pervasive in closed societies—assuming that the nation possesses the financial means to watch its citizens with electronic eyes. Certainly this was true in East Germany, by far the most prosperous nation in the history of communism, where per-capita incomes in the 1980s ran higher than those of non-communist Greece. The East German Stasi (short for das Ministerium für Staatssicherheit or Ministry of State Security) frequently monitored patrons of public lodgings through the use of a Czech-made surveillance camera with a German T1-340 lens. Made to fit into a special cylinder built into the hotel wall, the camera could be operated using a remote shutter release. This piece of equipment, used to spy on hotel patrons, was a variety of the German robot camera developed prior to World War II.

## Surveillance Cameras in Espionage

First used by the Nazis in 1934, the robot could snap multiple exposures without requiring manual winding. Originally used by the German air force to rapidly photograph the destruction of targets, it later became a favorite of Nazi intelligence services. The designs of the Nazi era culminated in the Star 50, which could snap 50 exposures in rapid succession. After the war, intelligence agents on either side of the Iron Curtain used robot cameras.

Made to be concealed and, if necessary, operated from a remote location, the robot was ideal for surveillance. Specific varieties of Star 50 were designed to be hidden in handbags, while the robot Star II was flat enough to fit in a special belt concealed by a trench coat. A false coat button covered the camera lens, and the manufacturers provided an entire matching set of buttons so that the user could replace those already on the trench coat if they did not match the false one. The robot Star II could also fit neatly into a briefcase.

The Soviet KGB developed their own variation on the robot, the F21, in 1948. Small—about the size of a hotel soap bar—and quiet, the F21 was ideal for concealment. At various times, Soviet designers adapted the F21 to hide it in belt buckles, jackets, umbrellas, and even camera cases. In the latter instance, the spy, posing as a tourist, would carry the camera case open and slung around the neck. The visible camera was a dummy; mounted on the side of the case was an F21 that took pictures at a 90-degree angle to the lens of the dummy camera.

Some other significant surveillance models in the history of Cold War espionage include the British Mark 3 automatic camera. Developed in the 1950s and still in use during the 1990s, the Mark 3 had a chamber so large it could hold enough film for 250 35mm exposures. Sometimes intelligence operatives needed moving pictures rather than stills, and for this, KGB relied on a movie version of the F21, developed in the 1960s. The camera was made to be hidden in a coat, using the false button technique applied with the robot camera.

**Copy cameras.** To copy documents, intelligence services required special cameras. An ordinary camera could theoretically be used, but would have difficulty in obtaining readable images. A much better option is to use a camera and accessories specially made for that purpose. A camera made specifically for copying documents has a high degree of photographic resolution, and is constructed in such a way as to be operated with a remote shutter release in order to avoid shaking the camera. Usually, the equipment would also include a stand of some kind that would both keep the camera steady and hold it fixed in place some distance from the documents being copied. Finally, because copying by an intelligence agent would most likely be a clandestine activity, it would be necessary to house all this equipment in a package that could easily be concealed.

One camera that fit the bill handsomely was built for the StB, the intelligence service of communist Czechoslovakia. Made to fit into an unobtrusive-looking wooden box, the kit included a Meopta copy camera, lights, a power plug, and a four-legged stand. The camera sat atop the stand, pointed downward. By pressing a button on a shutter release cable, the operator could photograph documents, which were illuminated by light bulbs fitted into housings at the base of the stand.

Both American and Soviet intelligence services used kits that resembled miniature copier machines. The American model was made to fit into an attaché case, while the Soviets' Yelka C-64 copy camera had the appearance of a thick book and, therefore, was unlikely to raise immediate suspicions.

Particularly ingenious was the Soviet rollover camera, disguised as a notebook. The undercover agent would regularly carry a real notebook to work, and use it often. Then, when it came time to make copies of documents, the agent would bring the rollover camera notebook, which was identical in appearance to the real notebook. In order to photograph a document, the agent would run the spine of the notebook carefully back and forth across the documents to be copied. Inside the spine were wheels that activated the camera, which was hidden, along with a battery-powered light source, inside the notebook.

**Working without a copy camera.** Perhaps the greatest resourcefulness of all was required for those situations in which the agent had no special equipment other than an ordinary camera. Victor Ostrovsky, of Israel's Mossad, developed a method for copying that used only a standard camera with a shutter release, a few thick books, and a couple of lamps. The document would be taped to the front of a book, which would be set standing on end, facing the camera. The latter would be placed atop one or more books lying flat, and fixed in place with an ordinary adhesive, such as chewing gum. On either side, desk lamps would provide concentrated lighting.

Another setup could be used when the agent needed to copy large amounts of documents, but could use only a camera and standard office equipment. Books would be stacked in two towers of equal height—perhaps 18 inches or so—with enough space between them to lay a document flat. Bridging the tops of the “towers” would be two parallel rulers, spaced almost the width of an ordinary 35mm camera. The camera would be taped to the rulers, and lamps placed on either side of the document. Then, documents could be run through one after the other, and a high volume of information recorded in a short time.

#### ■ FURTHER READING:

Babington-Smith, Constance. *Evidence in Camera: The Story of Photographic Intelligence in World War II*. Newton Abbott, England: David and Charles, 1974.

Melton, H. Keith. *The Ultimate Spy Book*. New York: DK Publishing, 1996.

Murphy, Dean E. “As Security Cameras Sprout, Someone's Always Watching.” *New York Times* (September 29, 2002).

Siljander, Raymond P. *Applied Surveillance Photography*. Springfield, IL: Thomas, 1975.

#### SEE ALSO

*Cameras, Miniature*

*Photo Alteration*

*Photographic Resolution*

*Privacy: Legal and Ethical Issues*

---

## Cameras, Miniature

---

### ■ JUDSON KNIGHT

Intelligence operatives frequently have a need for cameras that can be concealed, and while small size is not the only means to protect a camera from detection, it is certainly a significant one. Hence the value of small cameras such as the Minox, which could easily fit into the palm of a person's hand, as well as extremely small models no bigger than a thumb. During the years of World War II and the early Cold War, an age when cigarette-smoking was common, many spy cameras were designed to look like lighters, matchboxes, or cigarette packs. Some were made to photograph documents, others to photograph persons and buildings, while a special variety of cameras was applied to the copying of miniaturized photographic images via microdots.

## Concealment and Miniature Cameras

Concealment is often a concern for intelligence operatives using cameras. Sometimes a camera larger than miniature can still be concealed—even when in plain view. For example, the lens cap may be in place, so that observers would not think the camera was even taking pictures, but in reality the operator could be shooting exposures through inconspicuous holes in the lens cap, using a concealed shutter release. Or the apparent lens of the camera might be a dummy, and the real lens could be off to the side, at a 90-degree angle to the apparent lens.

The Soviet Tokya 58-M, while not miniature, was smaller than a pack of cigarettes, and made to be concealed behind the user's necktie. The agent would wear it strapped to his body, with the lens concealed behind a special tie pin. In order to ward off suspicion, the agent would make it a point to be seen often wearing an identical tie pin; then, when it was necessary to discreetly snap photographs, he could put the camera into place. The camera itself snapped pictures in almost complete silence, such that the sounds of a dinner party or a busy office





An Israeli miniature video camera of the 1980s. ©JEFFREY L. ROTMAN/CORBIS.

would be enough to conceal what little noise it made while operating.

Despite the variety of techniques for concealing cameras that are of ordinary size or very nearly so, in some instances it is preferable for an intelligence operative to carry a miniature camera. Some of these are small, and some very small: therefore it is common to speak of “miniature” and “subminiature” cameras. The distinction is a subjective one, however, and in both cases, the camera in question is so small that it must be constructed using principles somewhat different from those of a typical consumer camera.

## Design and Optics of Miniature Cameras

A miniature spy camera is almost completely lacking in the “frills” that one might expect from a camera built for ordinary use. Because of the size (and the need, in many cases, to prevent the camera from looking like a camera), there is almost never any viewfinder. The user must therefore be highly experienced at photography, so as to know

when an image is in focus without being able to actually see how it looks through the lens.

It is unlikely that a miniature camera, particularly those of the pre-digital cold-war era, would use color film, since this would simply constitute another frill and hence a complication in obtaining clear images. The film itself was usually smaller than 35mm: sizes ranging from 16mm all the way down to 9.5mm or smaller are typical of miniature and subminiature cameras.

**Lenses and light.** Virtually all cameras have at least one glass lens, and one with a zoom or telephoto lens typically has three: front and rear convex lenses, with a concave one in between. Though zoom lenses clearly have an application in the world of espionage, miniature and subminiature cameras are usually for photographing images at close range. Typically they would have only a single lens, perhaps with a coating to reduce reflections or glare.

An unusual example of miniature camera optics was the Soviet pinhole camera from the 1980s. One of the Soviet strengths in technology was the use of extremely simple, sometimes almost primitive, design to create extremely functional equipment that often outperformed its more complex and temperamental Western counterparts. Such was the case with the tiny camera, which was actually based on principles pioneered in the nineteenth century.

In place of lenses, a pinhole camera uses tiny apertures, or openings, so small that they are known as pinholes. The value of a lens lies in its ability to focus and thus photograph distant objects or ones close by, depending on the settings. By contrast, the value of a pinhole camera is precisely the fact that it does not have lenses, and therefore can produce images of distant and nearby images equally well.

Neither the faraway nor the closeup images produced by a pinhole camera have a very high degree of photographic resolution, and a photograph taken using this nineteenth-century technology will probably look like an old daguerreotype. But where clarity of image is not as important as versatility, quietness, and simplicity of design, a camera such as the Soviet model—so small it could be worn unobtrusively on a key chain—would be ideal.

**The Minox camera.** One of the great triumphs of miniature and ultraminiature design, applied for espionage work on both sides during the Cold War, was the Minox subminiature camera. Originally produced in 1938, it was the first significant and widely used miniature camera of the twentieth century. Small and flat, it could easily be concealed in the hand, yet for its size, it was exceptional in both its speed and the quality of the pictures it produced.

The designer of the Minox was Walter Zapp, a Latvian engineer who set out, not to make a tool of espionage, but rather to produce a camera that could be easily portable yet capable of producing photographs both quickly and

accurately. A Baltic German living in the Latvian capital of Riga, Zapp began producing his camera just before the Soviets annexed his country as an outgrowth of the 1939 non-aggression pact with the Nazis. Because of his German heritage, Zapp opted to move to his homeland, but it appears that the Nazis did not make use of his design. Therefore seven years elapsed between the production of the Riga Minox in 1938 and the founding of the Minox GmbH company in Germany. The latter produced more than 1 million cameras in its first half-century, and a 90-year-old Zapp was on hand for the company's 50th anniversary in 1995.

**Uses for espionage.** In the meantime, the Soviets, having appropriated Minox technology after capturing Riga, began producing their own miniature cameras. Among the Soviet spies associated with the Minox was John A. Walker, Jr., who used one given to him by his KGB handlers for photographing sensitive U.S. Navy and National Security Agency documents. After his arrest, Walker demonstrated for authorities how he used a Minox, along with a measuring chain to ensure that the camera was held a proper and uniform distance from the documents.

Western intelligence also recognized the value of the Minox, and its operatives continued to use them into the 1990s. Popular among both civilians and intelligence operatives was Model B, produced from 1958 to 1972, which was the first Minox with its own built-in light meter. It required no batteries, and therefore could be kept in hiding for many months until it was needed. As time passed, the resolution quality of Minox film improved dramatically, along with the enlargers used to make prints from the minuscule negatives produced by the camera. There were also improvements in the technology of developing film: thanks to a developing tank, it became possible to produce pictures without a darkroom, even in broad daylight.

## Other Notable Miniature Cameras

Today miniature and subminiature cameras are available for sale to civilian consumers via the Internet, but once these were virtually the sole province of intelligence services working on either side of the Iron Curtain. Today's designs for consumers—a jealous spouse, or an employer suspicious of employee malfeasance—are typically based on these old cold-war models.

As for the photographic technology utilized by today's espionage services, that information is unavailable to the general public. However, it is a safe guess that the technological gap between the equipment used by intelligence services and that used by amateur photographers is at least as great as it was in the middle of the twentieth century.

**Wristwatch cameras.** An example of a civilian product with a design related to that of a camera used in espionage is the

Tessina, still produced and sold by Concava SA of Switzerland. Unlike most tiny cameras, the Tessina, which is made to fit on a watchband, uses 35mm film, though this is loaded into special cassettes to make frames that measure just 14 x 21 mm. The Tessina was reportedly designed by Rudolph Steineck, whose Steineck ABC wristwatch camera is a classic of compactness in the service of espionage.

First produced in 1948, the Steineck ABC resembled a wristwatch, though it was not disguised behind a watch face. In fact, nothing about the Steineck looked like a watch except the size and the fact that it was attached to a watchband. Yet it bore such a close resemblance to a watch from a distance that it seldom attracted attention as a camera. The Steineck was capable of producing eight exposures, each about 6mm across, on a film disk that measured 25mm (some sources say 24) across.

**Cameras disguised as smoking paraphernalia.** One variety of Tessina used in the realm of espionage was a 35mm model, the smallest motor-driven camera of its kind in the world, which was designed to fit inside a cigarette pack. The shutter could be pressed from outside the pack, with very small holes on the exterior letting in just enough light to take pictures. The Tessina could shoot up to 10 exposures before it required manual winding.

Ingenuous as this Tessina model was, it simply fit inside a cigarette pack. By contrast, the Soviet Kiev 30 16mm model was actually designed to resemble a metal cigarette case, complete with dummy cigarettes. By moving one of the cigarettes, the user advanced the film and snapped pictures through a lens at the side of the pack.

During World War II, Eastman Kodak designed for the Office of Strategic Services a 16mm camera that was as small as a matchbox, and could be disguised as one simply by affixing a matchbox label. The lens opening was on the side, in a small hole on the striking surface, and the shutter release was at the end.

An early example of postwar Japanese technology was the Echo 8 cigarette lighter camera, which first appeared in 1951. It was even more authentic than the Soviet cigarette case or the American matchbox, because the lighter actually worked. In order to photograph the subject, the user simply flipped the top, revealing a viewing port and other equipment for a camera. It was a simple task to light a cigarette while snapping a picture from the side of the lighter. The "8" in its name referred to the 8mm film, made by slicing 16mm film down the middle.

**Microdot cameras.** Microdots were a specialized application for which certain cameras were used during the Cold War. This was particularly the case during the 1950s and 1960s, though microdots—tiny photographic images that require magnifying to be viewed—have been a fixture of intelligence work since the mid-nineteenth century. Microdots were ideal for passing messages between East and West

Berlin, for instance, a situation in which it was virtually impossible for agents to cross sides and pass documents without attracting attention. Instead, they could simply send mail containing microdots, which were so small that they would, in most instances, evade detection.

The East Germans designed a microdot camera about the size of the end joint on an average man's thumb. It could produce microdots smaller than a typical letter or character in a book. East German designers also created an ingenious microdot viewer that could be concealed in a fountain pen. Additionally, German intelligence services of both the Nazi and communist eras were known for their microdot concealment devices, which included a man's ring used in World War II (with the microdot hidden in a secret chamber atop the ring), as well as a postwar coin designed with a secret chamber.

#### ■ FURTHER READING:

##### BOOKS:

Babington-Smith, Constance. *Evidence in Camera: The Story of Photographic Intelligence in World War II*. Newton Abbott, England: David and Charles, 1974.

Melton, H. Keith. *The Ultimate Spy Book*. New York: DK Publishing, 1996.

Pritchard, Michael, and Douglas St. Denny. *Spy Camera: A Century of Detective and Subminiature Cameras*. London: Classic Collection, 1993.

##### SEE ALSO

*Photographic Resolution*

## Canada, Counter-Terrorism Policy

■ BRIAN HOYLE

Canada's measures to respond to or prevent terrorist activities have their origin in the October Crisis of 1970. At that time, a minister in the government of the Canadian province of Quebec and the British trade commissioner were kidnapped by members of a radical organization who advocated the separation of Quebec from Canada. The minister, Pierre Laporte, was killed by his captors.

One response of the federal government was to invoke an act of Parliament that temporarily revoked many democratic freedoms of Canadians in the interest of national security. As well, the Royal Canadian Mounted Police (RCMP) began a campaign of investigation and infiltration of the separatist organization and other perceived domestic terrorist organizations.

This counter-terrorism function shifted to the Canadian Security Intelligence Agency (CSIS) upon its establishment in 1984.

In the 1980s and 1990s, terrorism in Canada involved religious extremists (mainly Islamic groups), political activities surrounding the separation of states in India, Sri Lanka, Ireland, and the Middle East, and the activities of groups opposed to abortion, animal rights, and globalization. CSIS and other law enforcement agencies in the country assumed responsibility for the investigation of such incidents and prevention of further domestic violence. A full-scale government counter-terrorism policy did not yet exist.

The September 2001 terrorist attacks on the World Trade Center and the Pentagon in the United States prompted Canada to formulate policies to address the possibilities of terrorist movement through Canada to the U.S. and the presence of terrorist bases of operation in Canada. As well, Canadian officials were concerned that Canada might itself become a target of terrorism.

Canadian counter-terrorism policy involves several federal government departments and agencies. CSIS has assumed a prominent role in its capacity as an intelligence-gathering agency and as an advisor concerning possible national security threats. In the 1990s, some 80% of CSIS resources were devoted to counter-intelligence with only 20% dedicated to counter-terrorism. As of 2002, this ratio is reversed. Public safety has become the priority of CSIS.

The Threat Assessment Unit in the Counter-terrorism Branch of CSIS collects and evaluates information about domestic and international terrorism. This information is passed on to other government departments to initiate specific action (i.e., tightening of Canada-United States cross-border security by the departments of Citizenship and Immigration, and Transport). Information is also gathered prior to major international events to be hosted by Canada, which could become the target of terrorist activity.

CSIS, in combination with Citizenship and Immigration Canada, has tightened the screening of citizenship and refugee applicants, and has streamlined the review process for applicants in order to speed up approval or deportation. The rights of an applicant to appeal have been limited if their claim is rejected on their grounds of national security. Prior association with a recognized terrorist organization is a legal reason for refusal of entry to Canada and immediate deportation.

The United States-Canada border is the longest undefended national border in the world. Movement of terrorists across the border, particularly from Canada into the U.S., has not been difficult. As of late 2002, the Canadian government has taken steps to increase border security, searches of vehicles, and is developing joint strategies of border security with the United States.

Canada was one of the first countries to implement Resolution 1373 (2001) of the United Nations Security

Council, which required states to take action to prevent and suppress terrorism.

On October 2, 2001, the government of Canada implemented Resolution 1373. On October 15, 2001, the Antiterrorism Act was tabled in Parliament. The act (Bill C-36), which was passed in December 2001, amended the Criminal Code to restrict the ability of terrorists to finance their activities from Canada, restricted known terrorists from owning property in Canada, and increased the surveillance powers of the RCMP and CSIS. As well, stricter controls were put in place concerning the purchase and ownership of firearms.

Another piece of legislation, Bill C-42, proposes to amend the Immigration Act to allow the Minister of Immigration to approve the destination of anyone being deported. This would help ensure that the deportee did not escape to a jurisdiction that is sympathetic to their cause. The bill would also strengthen the search and seizure powers of customs agents at border crossings.

Objections to Bill C-42 concerning its infringement on civil liberties prompted its withdrawal and reformulation. New legislation called the Public Safety Act was introduced in April 2002. Among the recommendations is the coordination of federal and provincial government databases, to make a variety of information more widely accessible.

## ■ FURTHER READING :

### ELECTRONIC:

Canadian Security Intelligence Service. "Counter-Terrorism: Backgrounder Series No. 8." Government of Canada. August 8, 2002. <[http://www.csis-scrs.gc.ca/eng/backgrnd/back8\\_e.html](http://www.csis-scrs.gc.ca/eng/backgrnd/back8_e.html)> (26 November 2002).

Department of Foreign Affairs and International Trade. "Report of the Government of Canada to the Counter-Terrorism Committee of the United Nations Security Council on Measures Taken to Implement Resolution 1373 (2001)." Government of Canada. July 13, 2002. <<http://www.dfait-maeci.gc.ca/anti-terrorism/resolution1373-en.asp>> (26 November 2002).

### SEE ALSO

*Airline Security*  
*Canada, Intelligence and Security*  
*Information Security*

## Canada, Intelligence and Security

### ■ BRIAN HOYLE

As of July 1984, Canadian security and intelligence operations have been the responsibility of the Canadian Security Intelligence Service (CSIS). The Canadian Security

Intelligence Service Act legislated the formation of CSIS as a replacement for the Security Service, which was part of the Royal Canadian Mounted Police (RCMP).

In 1984, Canada was one of only a few western democratic nations to have a legislated security and intelligence force, with mandated boundaries to the scope of its operations and a monitoring process to ensure that the agency operates as intended. The Federal Bureau of Investigation in the United States is another example of a security and intelligence gathering agency with a conceived purpose and mandate.

Up until the mid-1970s, the task of defining what was to be considered a security risk to Canada and monitoring security developments was the responsibility of the RCMP. The force's Security Service performed security and intelligence gathering functions for the country. At that time, the perceived threat from other nations or organizations was ill defined, and no government security policy was in force. The operations of the Security Service had evolved over time and were the sole responsibility of the RCMP. Decisions regarding the targets of intelligence gathering were the domain of the Security Service. As a result, the government and the citizens of Canada had little knowledge of the measures being taken by the RCMP in the areas of national security and intelligence gathering.

**Canadian security agency history.** The roots of Canada's intelligence and security agencies date back almost 150 years, to the Royal Canadian Mounted Police Act of 1864. At that time, Canada had not formally become a country. A number of police forces operated in various regions of what, three years later, would become Canada. In 1864, Sir John A. MacDonald—the prominent political figure of the day and the man who would become Canada's first Prime Minister—assigned certain responsibilities to what was then called the Dominion Police Force. Security related duties included safeguarding the federal government's parliament building and collecting information concerning perceived security threats to Canada (i.e., at that time, the government was wary that the Fenians—a group of Irish nationalists who advocated for the political separation of Ireland from England—were planning to invade Canada from the United States).

The intelligence and security role of the Dominion Police Force increased in scope in 1920, when the Dominion Police joined with another force called the Royal North West Mounted Police (who operated in the western region of the country) to form the RCMP.

Having assumed the role as the country's intelligence and security agency, the RCMP's role and focus shifted over time in response to national priorities. For example, by the time of World War I, the RCMP was actively responding to labor unrest, which was perceived as being anarchist and of Communist origin, and so was viewed as a national security threat.

In 1920, the RCMP's security role was officially sanctioned with the formation of the Criminal Investigation

Branch. By the early 1940s, the focus of the Criminal Investigation Branch shifted yet again. Then, in the climate of escalating tensions between the former Soviet Union and the democracies of the western world, the existence of Soviet espionage networks in Canada became known. In 1946, largely in response to these tensions, an official branch of the RCMP dedicated to security and intelligence gathering was created and termed the Special Branch.

**From the Special Branch, to the Security Service, to CSIS.** Over the intervening decades, the relatively free hand that the RCMP exercised in national security created an atmosphere conducive to excessive and inappropriate behavior. For example, by the 1960s the RCMP was conducting surveillance campaigns on university campuses across Canada, having been convinced that campuses were fostering social unrest. Entertainment personalities and the even the country's tax payer-funded national radio and television system, the Canadian Broadcasting Corporation, were targeted for the same reason. Indeed, by the late 1960s the RCMP had investigated over 800,000 Canadians for evidence of Communist connections. Additionally, during the 1960s and 1970s, the Special Branch had adopted illegal methods—including theft, break-ins and property damage—to obtain information and foster dissension among groups considered to be security threats.

Recognizing the need for reform of the security framework in the country, the federal government of the day undertook an exhaustive analysis of the RCMP's security framework (in Canada these analyses are termed Royal Commissions). The Report of the Royal Commission on Security was released in 1969. The report recommended that national security should part of a civilian agency and part of the mandate of the country's federal police force.

The government responded in 1970 by forming the Security Service, which, while still part of the RCMP, was "civilian in nature", according to then Prime Minister Pierre Elliot Trudeau. For example, the Director General of the service was a civilian. In reality, however, the bulk of the Security Service was composed of RCMP officers and little changed in the intelligence and security operations community.

In October 1970, a minister in the government of the province of Quebec and the British trade commissioner to Canada were kidnapped by members of a group advocating separation of Quebec from Canada. The minister, Pierre Laporte, was murdered. In the aftermath of these events, the lack of information concerning the radical separatist movement became apparent, as did the illegal nature of some of the Security Service's intelligence gathering activities. The federal government was galvanized into revamping the Security Service. Another examination of national security was commissioned. The MacDonald report, which was released in 1981, echoed the earlier Royal Commission report in calling for a civilian security agency.

In May 1983, the Canadian government introduced Bill C-157, legislation that would create CSIS. This bill proved controversial, with many challenges arising concerning the possible infringement on civil liberties. After revision, Bill C-9 was proclaimed law in July and August, 1984. The responsibility for Canadian security measures and intelligence gathering passed from the RCMP's Security Service to CSIS.

**The Mandate of CSIS.** The legislation that created CSIS mandated the agency to function as a clearinghouse for security information. In other words, CSIS investigates perceived security threats to Canada and, if warranted, collects, analyzes, and compiles information on the security threats. The agency is able to provide advance warning to various government departments and agencies of individuals or activities that are suspected of being national security threats. The agency's powers end there. CSIS does not have any law enforcement responsibilities. If a department requires further information, CSIS can have an ongoing role in the process.

The legislation that spawned CSIS also mandated the types of security threats that the agency could respond to. Potential security threats take four forms. The first is espionage or sabotage that is actively directed against Canada or either threatens the country's own intelligence gathering efforts or other national interests. An example of such a threat is the gathering of economic, military, or scientific information by a group or government in a way that is illegal or unauthorized.

The second category of security threat involves activities originating in another country that threatens Canadians or the country's interests. An example would be the pressuring of an ethnic community by a foreign organization or government seeking the community member's participation in a terrorist conflict in the home country.

In the third category, security threats originate from within the country. Hostage taking (e.g., the separatist kidnappings of 1970), bomb threats or bombings, and politically motivated violence could threaten the security of Canadians. Also in this category is the use of Canada as a haven for terrorist activities in other countries. The alleged existence of Al-Qaeda terrorist cells in Canada is a current example of a security threat that CSIS is mandated to explore.

Finally, subversive threats to various levels of government in Canada and the country's judicial and economic system are potential security threats.

**Regulation of security and intelligence in Canada.** CSIS is subject to regular review and monitoring of its procedures and activities. The act that spawned CSIS also created the office of the inspector general and the Security Intelligence Review Committee (SIRC). The inspector general monitors CSIS operations and reports on whether these operations are legal or appropriate to the deputy solicitor

general (the second most powerful law enforcement officer in the country) and the SIRC. The SIRC is composed of five people who are selected following consultations with the prime minister and the leaders of all the qualified opposition parties in the House of Commons. The SIRC also conducts a review of CSIS activities and operations each year and reports its finding to the ministers of defense and foreign affairs, and to Parliament. By reporting to Parliament, the fullest public disclosure of the SIRC reports are ensured.

A caveat to the full and open disclosure of information, however, is the denial of cabinet documents to both the inspector general and the SIRC. Thus, some information about CSIS operations is kept secret.

The covert nature of some of Canada's intelligence and security network has been contentious from the establishment of CSIS. Much of the debate surrounding the formation of CSIS centered on its mandate. The idea that the country's security force would have full authorization to deal with "subversion" and "foreign influenced activities" struck some critics as too broad and hazy a frame of reference. Civil libertarians, in particular, argued that the lack of precision in the mandate could allow CSIS to legally infringe on the civil right of Canadians.

The regulatory and monitoring processes seek to minimize these civil rights issues. In response to a legal challenge, the Federal Court of Appeal ruled in 1987 that the Canadian Security Intelligence Act does not violate the Canadian Charter of Rights and Freedoms.

**The powers of CSIS.** The security and intelligence functions of CSIS apply only within the borders of Canada. Foreign intelligence, including offensive operations in other countries, is not part of the mandate of CSIS.

The federal government guides the powers that CSIS wields. Thus, the direction of the agency can change. This has occurred as the global tensions between the Eastern Europe and the West have declined, and as terrorists operations have escalated. CSIS is now concerned primarily with preserving the national security from disruption from within the country than from beyond Canada's borders. Operationally, the solicitor general, a member of the governing party who is the overseer of CSIS, provides government direction.

Intelligence information is gathered from a wide variety of sources, both public and privileged. Public sources include newspapers, trade journals, periodicals, academic journals, radio and television broadcasts in Canada and abroad, and via official government documents. Privileged sources include the interception of telecommunications.

The information that is collected is analyzed by the field staff who collect it and by personnel at CSIS headquarters. The information can be combined with other information to provide a national picture of the significance of the suspected security threat. The final step is the

release of the analysis to the concerned government departments.

One of the main analysis reports is known as a threat assessment. Different departments use the threat assessment to determine responses. For example, the RCMP can use a threat assessment to gauge the degree of security provided to a visiting dignitaries and to prominent Canadians traveling abroad. As another example, the Department of Foreign Affairs and International Trade will use a threat assessment report to provide the proper security to Canadian business and governmental missions in foreign countries. Transport Canada also uses the assessment to issue warnings to the general public about travel.

As of late 2003, the primary role of CSIS is the safety of Canadians from security threats. This includes terrorist activity. As such, much of the information that CSIS collects on terrorist activities is shared with security and enforcement agencies in other countries including the United States.

## ■ FURTHER READING:

### BOOKS:

Cleroux, Richard. *Official Secrets: The Story behind the Canadian Security Intelligence Service*. Toronto: McGraw-Hill Ryerson, 1990.

Hewitt, Steven. *Spying 101: The RCMP's Secret Activities at Canadian Universities*. Toronto: University of Toronto Press, 2002.

Starnes, John. *Closely Guarded: A Life in Canadian Security and Intelligence*. Toronto: University of Toronto Press, 2001.

### PERIODICALS:

Farson, S.A. "Is Canadian Intelligence Being Re-Invented?" *Canadian Foreign Policy* no. 6 (1999): 49-83.

### ELECTRONIC:

Canadian Security Intelligence Service. "A Historical Perspective on CSIS." Government of Canada. November 01, 2001. <[http://www.csis-scrc.gc.ca/eng/backgrnd/back5\\_e.html](http://www.csis-scrc.gc.ca/eng/backgrnd/back5_e.html)> (06 December 2002).

Library of Parliament. "The Canadian Security Intelligence Service." Parliamentary Research Branch. January 24, 2000. <<http://www.parl.gc.ca/information/library/PRBpubs/8427-e.htm>> (06 December 2002).

## Canine Substance Detection

■ JUDYTH SASSOON

Canine substance detection involves the use of specially trained dogs, commonly golden or Labrador retrievers, for the detection of illegal substances. Dogs of this kind are now being used in various different situations, such as



John Long and his bomb-sniffing dog Coby check luggage as they go through a drill at Lackland Air Force base in San Antonio, Texas, in February 2002. AP/WIDE WORLD PHOTOS.

workplaces, airports and schools, to detect weapons, contraband, narcotic drugs, abused medication, alcohol, firearms and explosives. The necessity for this is due, in part, to the increasing incidents of drug abuse and violence among young people and employees, along with a growing need for increased security in schools and workplaces. Many schools and employers in the United States are now engaging “sniffer dogs” to improve safety and assist in the prevention of drug abuse. Supporters of this policy argue that the presence of these dogs, even if they do not immediately turn up illegal substances, provides a powerful deterrent. There are also, however, a number of school principals and employers who are concerned about this method because they anticipate that the seizure of illegal substances would reflect badly on their institutions and companies. Nevertheless, the reality is that today narcotic drugs, alcohol, and weapons are discovered in schools and in addition account for an astonishing 70 percent of injuries at work.

Dogs trained to detect the scent of illegal substances are useful as they can utilize their acute sense of smell to penetrate many hiding places which are inaccessible to

other detection methods. A dog has about 200 million sensitive cells in its nose, compared to about five million or so in a human being, and therefore, a dog’s olfactory system is around 40 times more sensitive than that of a human. A dog’s sense of smell is made even keener by an organ in the roof of the mouth that is not found in the human olfactory system and this enables it to “taste” a smell, amplifying a weak smell into a stronger one. This sensitivity to, for example, the odor of butyric acid emitted in sweat, enables a dog to locate an object, such as a ball, belonging to its owner from several similar objects thrown by a number of different people. It also enables tracking dogs such as bloodhounds to pursue and keep pace with a fugitive for up to 100 miles. Dogs also have the ability to distinguish individual odors when other strong smells are also present. They can be trained to detect the odors of heroin, marijuana and cocaine hidden in suitcases even in the presence of strong smelling perfumes. Drug traffickers are constantly attempting to find more sophisticated ways of smuggling illegal drugs and the scenting abilities of sniffer dogs often provide the only means of locating well-hidden narcotics. Canine drug detectors have proved so

successful that they are now employed in many airports and also at bus stations, border crossings, and ports. The dogs are trained both to detect the drugs and then to alert authorities, either by pawing at the surface near the location of the smell or by sitting down next to the source. This behaviour usually provides the authorities with a valid cause to search luggage or vehicles.

Trained detection canines were introduced into American public schools in Texas in the 1980s. The concept soon became popular and widely used as a tool for increased safety and as a drug deterrent on campuses. Thus, drug and narcotic detection are today an important aspect of school security. Also, because of the increasing danger of violence in schools, weapons and contraband detection also plays a role in the promotion of school safety. Depending upon the school or business, a program of regular canine visits is developed to detect illegal substances or weapons. Typically, everyone is informed about the pending visit of a sniffer dog and in most cases, the dogs are allowed to meet the students and employees beforehand. Subsequently, the dogs are brought in with a handler on a random, unannounced basis and perform "spot checks" on designated areas.

Some dogs are specially trained to detect the acidic smell of nitroglycerin and the sulphur in gunpowder for work with explosives detection. Fire investigators use arson dogs to help in criminal investigations. These canines locate minute traces of gas or other flammable liquids in situations where arson is suspected. Arson dogs are trained in such a way that they can accurately detect traces of arson about the size of a thousandth of a drop, which is much more efficient than any commonly used electronic detection device.

In 2002, it was reported that scientists at Russia's DS Likhachev Scientific Research Institute for Cultural Heritage and Environmental Protection successfully bred a new kind of highly efficient sniffer dog. The new breed is a cross between a wild jackal and a Russian husky. The breeding program was started in 1975, and in 2002, the institute successfully produced hybrids that were a quarter jackal and three-quarters husky. These hybrids were bred to combine the very sensitive nose of the wild, scavenging jackal with the more benign temperament of the husky. The jackal has a sense of smell that is even keener than that of its domestic counterpart. It was reported that many dog species are losing their naturally sharp sense of smell through domestication. Huskies are used as the domesticated breed in this program because they have a better developed sense of smell than all other dog breeds. This is because they are adapted to severe conditions of arctic cold where many substances become non-volatile and exist in only a highly diluted form. This crossing of highly sensitive canines has produced a breed that is now being used by authorities at Russian airports. By 2003, some twenty-five of the dogs were employed at Sheremetyevo Airport, Moscow and ten more were working at the forensic criminology examination department nearby. Their handlers reported that, aside from their

sharp sense of smell, the jackal hybrids were also highly courageous and expert at crawling into the tightest corners, especially during the inspection of aircraft.

#### ■ FURTHER READING:

##### BOOKS:

Tonry, Michael *Malign Neglect: Race, Crime, and Punishment in America*. Oxford University Press, 1996.

##### PERIODICALS:

Charles Mesloh, Ross Wolf and Stephen Holmes. "A Pilot Study of the Confounding Effects of 'Jute' on Law Enforcement Canine Training." *Journal of the Academy of Canine Behavioral Theory* 1 (2002): 2–9.

##### ELECTRONIC:

United States Department of Agriculture. "The AQI Program at Airports." <<http://www.aphis.usda.gov/oa/pubs/detdog1.html>> (February 20, 2003).

##### SEE ALSO

*Airline Security*  
*Drug Control Policy, United States Office of National*

## CAPS (Computer Assisted Passenger Screening System).

SEE *IBIS (Interagency Border Inspection System)*.

## Carnivore Program.

SEE *Internet Surveillance*.

---

# Carter Administration (1977–1981), United States National Security Policy

---

■ CARYN E. NEUMANN

While President Jimmy Carter notably became the first president to label access to Middle Eastern oil as a vital security interest, his single term in office is widely viewed with skepticism in terms of national security. Carter's micro-management and concomitant power struggles within the administration did little to arrest the sharp decline in American power and influence that occurred in the 1970s.





United States President Jimmy Carter, left center, and Soviet President Leonid Brezhnev, right center, shake hands amidst applause in the Vienna Imperial Hofburg Palace after signing the SALT II treaty, June 8, 1979. AP/WIDE WORLD PHOTOS.

In the 1976 presidential election, the Democrats chose Carter, a one-term governor of Georgia as their standard bearer specifically because he could capitalize on the post-Watergate cynicism about politicians. A graduate of the United States Naval Academy, a born-again Baptist, and a peanut farmer, the folksy Carter spent the campaign stressing both his honesty and his lack of inexperience in the byways of Washington politics. He promised to use his engineering education and his experience as an officer on a nuclear submarine to be a hands-on manager who would establish systemization in government. In office, Carter's strong concern with the minutiae of administrative procedure left him less able to assume the chief leadership role among top levels of government.

Carter sought to avoid the extreme centralization of power that had characterized the Nixon administration's security policy. He expected to serve as a policy initiator and manager who would make decisions from the range of views presented to him by his senior advisors. He saw Secretary of State Cyrus Vance as the principal advisor for foreign policy, while the National Security Council would play a less active and assertive role than in previous administrations. In practice, the Carter administration had two secretaries of state. National Security Advisor Zbigniew Brzezinski, a man accustomed to aggressive debate, proved

particularly adept at gaining the president's confidence. He also became an outspoken advocate of the administration's security policy. Vance publicly competed with Brzezinski for the position of chief presidential advisor, a situation that left some congressional members confused about the chain of authority. Vance ultimately resigned in 1980 in protest over the failed rescue attempt of the American hostages held by Iran. His replacement, Edmund S. Muskie, had too brief a term to make a significant impact.

While suffering from management strategy weaknesses, the Carter administration may have been troubled from the start by growing problems facing the United States. Dwindling resources had led to a severe energy crisis that worsened when renewed violence struck the Middle East. This situation prompted Carter to issue a new foreign policy declaration that marked energy as a matter of national security. The Carter Doctrine stated that the United States would employ force if necessary to protect its continued access to the oil fields of the Middle East. The administration also pushed for the development of synthetic fuels, but Congress only partially funded this request.

Like Nixon and Ford before him, Carter attempted to reduce tensions with the Soviet Union. The controversial Strategic Arms Limitation Treaty (SALT II) was similar to SALT I in that it did not do much to slow down the nuclear



Despite President Jimmy Carter's (shown here with his advisors) efforts to resolve the Iranian hostage crisis, 52 Americans were held at the American embassy in Teheran, Iran for 444 days. January 20, 1981. ©BETTMANN/CORBIS.

arms race. The agreement placed a ceiling of 2,250 bombers and missiles on each side and set limits on the number of warheads and new weapons systems. In order to ensure that the Soviets did not gain an advantage in the number and destructive power of land-based missiles, Carter proposed the MX missile system. The system proposed to befuddle the Soviets and prevent them from successfully launching an attack by moving the MX missiles around a vast maze of underground tunnels connected by a railroad. While the Senate debated the merits of SALT and the MX, the Soviets invaded Afghanistan. Carter immediately shelved the treaty.

Carter's presidency would be further weakened when the Iranian hostage crisis in 1979 exposed the inability of the U.S. to control world affairs. Carter appealed to the United Nations for help but the head of Iran, Ayatollah Ruhollah Khomeini, ignored the U.N.'s requests. Carter then froze Iranian assets and imposed a trade embargo. Americans clamored for a military response, which Carter eventually provided by sending commandos to Iran in

1980. The raid was aborted by helicopter failures that left eight soldiers dead. The crisis finally ended after 444 days when Carter released Iranian assets to ransom the 53 hostages.

#### ■ FURTHER READING:

##### BOOKS:

Carroll, Peter N. *It Seemed like Nothing Happened: America in the 1970s*. New Brunswick: Rutgers University Press, 1990.

Crabb, Cecil V. and Kevin V. Mulcahy. *American National Security: A Presidential Perspective*. Pacific Grove, CA: Brooks/Cole, 1991.

##### SEE ALSO

*ADFGX Cipher*  
*Cold War (1972–1989): The Collapse of the Soviet Union*  
*Eisenhower Administration (1953–1961), United States National Security Policy*

*Middle East, Modern U.S. Security Policy and Interventions  
National Security Advisor, United States  
Nixon Administration (1969–1974), United States National  
Security Policy*

## Case Officer.

SEE *Intelligence Officer.*

## CDC (United States Centers for Disease Control and Prevention)

■ BRIAN HOYLE

CDC is an acronym for Centers for Disease Control and Prevention. The center, which is headquartered in Atlanta, Georgia, is one of the predominant public health institutions in the United States and in the world. The CDC serves United States national security by monitoring the incidence of infectious disease in the U.S. (and around the world), and through the development and implementation of disease control procedures. As part of this mandate, the CDC is one of the few facilities in North America that houses a biological laboratory capable of handling very infectious and lethally-dangerous microorganisms such as the Ebola virus and *Bacillus anthracis*, the bacterium that causes anthrax.

The CDC is the pre-eminent institution in the United States dedicated to the prevention of disease, and is a global leader in public health. In addition to the Atlanta headquarters, the CDC has facilities in San Juan, Puerto Rico, and in eight other locations in the continental United States. The U.S. locations are Anchorage (Alaska), Cincinnati (Ohio), Fort Collins (Colorado), Morgantown (West Virginia), Pittsburgh (Pennsylvania), Research Triangle Park (North Carolina), Spokane (Washington), and Washington D.C.

Approximately 8,500 people work at the CDC in 170 occupations pertaining to public health research, administration, monitoring, and education. CDC personnel are also seconded to other international health agencies such as the World Health Organization and to state and local health agencies in response to disease outbreaks.

The CDC is organized into 11 national centers that are concerned with health care and disease prevention. The national centers study:

- Birth Defects and Developmental Disabilities,
- Chronic Disease Prevention and Health Promotion,

- Environmental Health (that includes the Office of Genomics and Disease Prevention),
- Health Statistics
- HIV (Human Immunodeficiency Virus), STD (Sexually Transmitted Disease), and TB (Tuberculosis) Prevention,
- Infectious Diseases,
- Injury Prevention and Control,
- Immunization Program,
- Occupational Safety and Health,
- Epidemiology Program, and,
- Public Health Practice Program.

At the beginning of 2003, the CDC enters its 57th year of existence. The institution was established on July 1, 1946 in Atlanta. At that time the acronym CDC stood for Communicable Disease Center. The CDC replaced another center known as the Malaria Control in War Areas. The former institution had been established as part of the Public Health Service to rid the southern United States of malaria during the years of World War II. As well, the center had assumed the responsibility for keeping the region free of murine typhus fever. The establishment of the Communicable Disease Center continued these functions while expanding to include all diseases that could be transmitted from person to person.

The institute's founding director was Dr. Joseph M. Mountin. In its early days, the center was small and research and surveillance programs were still geared towards insect-transmitted diseases such as malaria. After an aggressive campaign of expansion by Mountin, however, which was intended to entrench CDC's position and value to the country, the center became the national agency for epidemiology (the study of the origin and spread of diseases).

The Korean War in the 1950s solidified the center's value as an epidemiological resource. The Epidemiological Intelligence Service (EIS) was created during that time, with the mandate to protect U.S. citizens from diseases that originated in other regions of the world. The EIS remains an important part of today's CDC, especially because of the recognition, in the 1950s, that biological warfare was an emerging threat to national security.

Two other events in the 1950s besides the Korean conflict increased the national importance of the CDC, and served to ensure that the funding of the center continued. First, a national campaign to inoculate children with the recently approved Salk polio vaccine led to a spate of poliomyelitis cases. A Polio Surveillance Unit was established at CDC. The unit quickly determined that a contaminated batch of the vaccine has been the problem. Their findings allowed the contaminated units of vaccine to be withdrawn from use, and the inoculation program continued with confidence. In retrospect, the continuation of the vaccination campaign has been invaluable, since it was pivotal in the eradication of polio, and since it instilled the confidence in vaccines in general that helped ensure the



In one of the biggest steps taken towards modernizing defenses against smallpox, the Centers for Disease Control (CDC) dedicated one of its two maximum containment laboratories to smallpox-only research in 2002. A senior researcher is shown through a glass viewer entering the Biosafety-Level-4-Lab wearing a biohazard protective suit. AP/WIDE WORLD PHOTOS.

success of other vaccination campaigns. These outcomes also solidified the CDC's reputation as a disease-monitoring center of excellence. The other event was a large influenza outbreak in the U.S. Once again, a surveillance campaign on the type of virus that was involved and its pattern of spread helped future efforts to develop effective vaccines and inoculation programs.

During the 1950s and 1960s, the CDC grew through the assumption of responsibility for programs that had been previously handled by other government departments and agencies. Examples include the centers of venereal disease, tuberculosis, and immunization.

Beginning in the 1960s, CDC assumed an increasingly important role in the public awareness of infectious diseases. One important example occurred in 1961 when the institution took over the publication of the *Mortality and Morbidity Weekly Report* (MMWR). The MMWR publishes information on the number of deaths and cases of infectious disease from every state in the country each week. The availability of such detailed information has allowed the progression of some emerging diseases such as AIDS to be charted.

By the late 1960s, the CDC had become much more than a center for the study and action against communicable diseases. These activities had moved CDC far beyond its original mandate as a communicable disease center. In recognition of the center's changed role, its name was changed in 1970 to the Center for Disease Control. Further expansion led to a slight name change in 1981, to the Centers for Disease Control. Finally, as further expansion took the CDC into disease prevention, in 1992 the organization became the Centers for Disease Control and Prevention. Even so, for the sake of continuity the acronym CDC has been retained.

These and other efforts have contributed to national security through the preservation of public health. In more recent times, accomplishments of significance have included participation in the development of a smallpox vaccine and inoculation program, and the identification of the agents of several diseases including Legionnaire's disease, toxic shock syndrome, hantavirus pulmonary syndrome, and Acquired Immunodeficiency Syndrome.

In 1978, biosafety level 4 containment laboratory was opened in the CDC Atlanta headquarters. Then as now, this is one of only a handful of level 4 labs in North America. Other similar facilities are present in San Antonio, Texas, at the U.S. Army Medical Research Institute of Infectious Disease (USAMRIID) in Fort Detrick, Maryland, and in Winnipeg, Manitoba, Canada. It is only at these facilities that highly infectious and lethal viruses and bacteria can be safely studied and treatments devised. At CDC, for example, the Special Pathogens Branch studies the Ebola, Marburg, and Hantaviruses.

In the present day, CDC provides a great deal of information concerning naturally occurring infectious diseases and, particularly since in the aftermath of the September 11, 2001 terrorist attacks on the U.S., information

on bioterrorist threats such as anthrax. The research and disease surveillance expertise at CDC is being harnessed, along with other national laboratories and intelligence gathering organizations, to strengthen the United States from bioterrorist attacks.

#### ■ FURTHER READING :

##### PERIODICALS:

Epidemiology Program Office, CDC. "CDC's 50th Anniversary: History of CDC." *Morbidity and Mortality Weekly Report* no. 45 (1996): 525–30.

##### ELECTRONIC:

Centers for Disease Control and Prevention. "About CDC." November 2, 2002. <<http://www.cdc.gov/aboutcdc.htm>> (28 December 2002).

Centers for Disease Control and Prevention. "CDC Timeline." <<http://www.cdc.gov/od/oc/media/timeprnt.htm>> (28 December 2002).

##### SEE ALSO

*Biocontainment Laboratories*  
*NNSA (United States National Nuclear Security Administration)*  
*Public Health Service (PHS), United States*

---

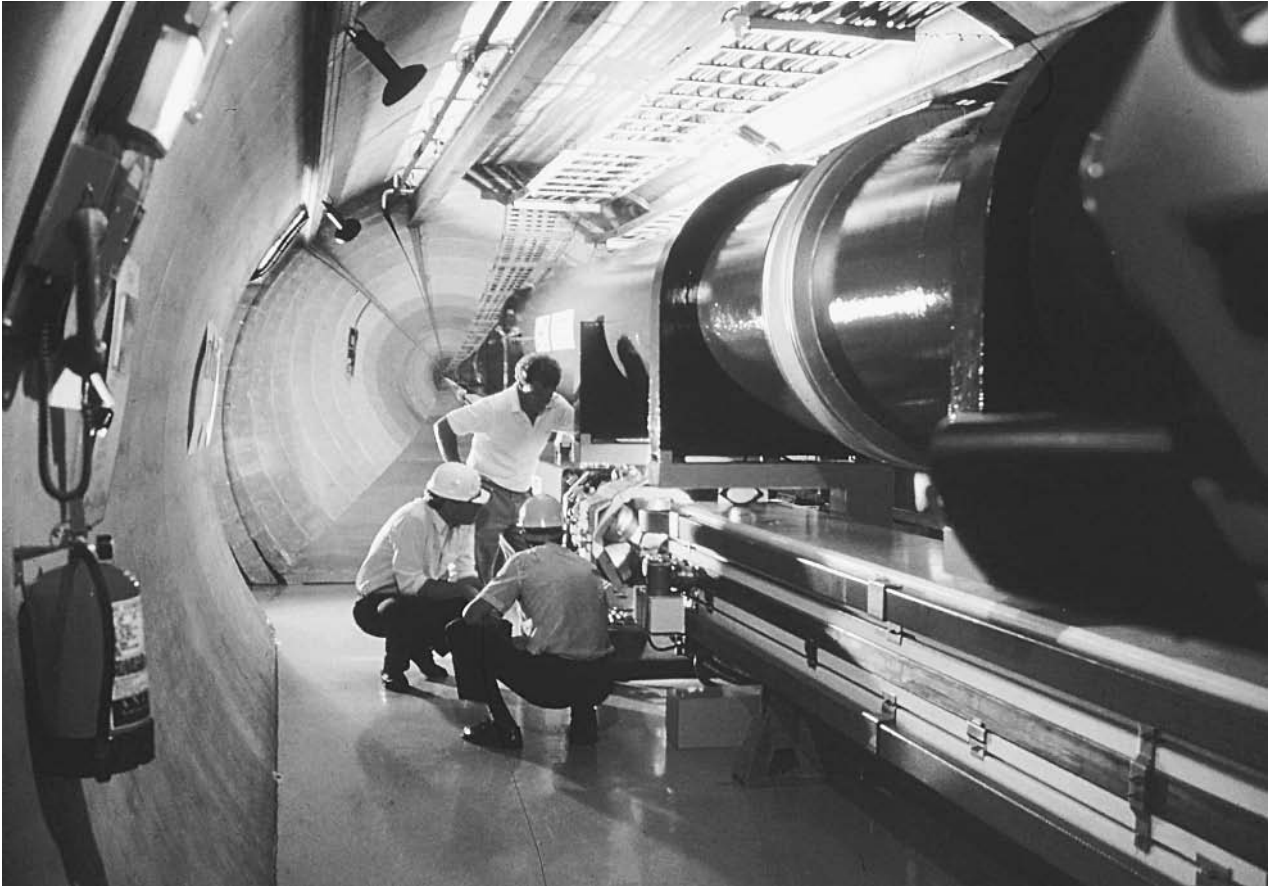
## CERN

---

#### ■ LARRY GILMAN

CERN, located along the French-Swiss border near the Swiss capital Geneva, is the world's largest particle-physics laboratory. (The acronym stands for Conseil Européenne pour la Recherche Nucléaire, French for CERN's original name, the European Council for Nuclear Research; since October 1954, despite retention of the old acronym, CERN's name has actually been *Organisation Européenne pour la Recherche Nucléaire*.) CERN was founded in 1954 and today is supported by a consortium of 20 European nations and by a number of "observer states," including Japan and the U.S. Besides being responsible for many fundamental discoveries in particle physics, primarily through the use of particle accelerators, CERN is the birthplace of the World Wide Web.

CERN is a non-military organization; Article II.1 of the multinational convention establishing the laboratory states that it "shall have no concern with work for military requirements and the results of its experimental and theoretical work shall be published or otherwise made generally available." However, CERN is unavoidably relevant to



Mock-up of the CERN Large Hadron Collider or LHC atom-smasher under construction in a 27-kilometer tunnel near Geneva. ©AFP/CORBIS.

military affairs via the relevance of all physics to military affairs. The proposal in 1949 to form a regional European physics laboratory (i.e., CERN) was directly inspired by the explosion by the Soviet Union, in that year, of its first atomic bomb; furthermore, while CERN was being founded during the early 1950s, the building of particle accelerators in the United States was funded primarily by the military, which hoped to produce particle-beam weapons and to manufacture polonium for radiological warfare (i.e., the use of radioactive dust as a weapon). Both scientists and politicians involved in the founding of CERN were, therefore, aware that military applications of research in particle physics, though not predictable, might eventually occur. Furthermore, the advanced scientific equipment and techniques that would be developed at CERN and the large pool of expertise it would create and sustain were seen as basic military European assets. Likewise, the U.S. Navy's Office of Naval Research financed research in fundamental physics in U.S. universities in the postwar years on the ground that even "untargeted" research—science for science's sake—could, on average, ultimately be counted on to bear military fruit.

Nevertheless, CERN is as non-military, non-secretive, and international as an institution could well be. The

construction of a nuclear reactor at CERN was ruled out from the beginning precisely because of the obviously military applications of such technology. CERN has therefore focused on the use of particle accelerators for research, avoiding the production or use of militarily significant amounts of fissionable materials and leaving the military implications (if any) of its discoveries to be worked out by national and commercial laboratories. To further distinguish it from a weapons-research laboratory, CERN does not classify any of its results, but, in accordance with its founding convention, makes them openly available to all inquirers.

Design work for CERN's first facilities proceeded in Geneva, Switzerland during 1953 and 1954 while the final international agreements were being worked out by CERN's original 11 member states. Construction contracts were awarded in October 1954, and CERN's first accelerator, a 600 MeV proton synchro-cyclotron, began operation in 1957. Confirmation of pion decay was one of the first experimental results, beginning a long line of important physics results made at CERN.

Not all of CERN's contributions have been in the realm of physics; in 1990, CERN computer scientists Tim Berners-Lee and Robert Cailliau proposed a network of

“hypertexts” (texts, images, and other information objects linked by computer addresses routinely hidden from the user) that would run on computers connected through the Internet, which was already used for file transfers, e-mail, and other purposes. They proposed that this network be called the World-Wide Web, a name which has stuck.

Approximately 6500 physicists from 80 countries work at CERN, which operates a number of particle accelerators and detectors. CERN’s largest tool is a circular particle accelerator 16.7 miles (27 km) in circumference, located some 320 feet (100 m) underground. CERN can achieve higher particle energies than any other facility in the world, making it a key facility for ongoing advances in particle physics.

#### ■ FURTHER READING:

##### BOOKS:

Hermann, Armin, et al. *History of CERN*. Amsterdam: North-Holland Physics Publishing, 1987.

##### ELECTRONIC:

“The CERN Archive.” February 12, 2002. <<http://library.cern.ch/archives/index.html>> (March 11, 2003).

## Chain Reaction.

SEE *Nuclear Reactors*.

## Chatter.

SEE *Electronic Communication Intercepts, Legal Issues*.

---

## Chechen-Russian Conflict

---

#### ■ JUDSON KNIGHT

During the 1990s, westerners became aware of a seemingly incongruous conflict between the Russian Federation and Chechnya, a small breakaway republic along its southern border. In fact, Chechens had resisted Russian rule, sometimes actively and sometimes passively, for over two centuries. To both sides, as well as to outside observers, the success of the Russian response to the secessionist movement served as a litmus test for the

Kremlin’s ability to maintain sovereignty over Russian territories in the post-Cold War era.

## Background (1791–1991)

Located along the northern flank of the Greater Caucasus mountain range, Chechnya is about the size of Massachusetts, with a much smaller population: about 1,165,000 people at the end of the twentieth century. To the east and southeast is Dagestan, which, like Chechnya, was an outlying minority region of the Russian Empire in the eighteenth and nineteenth centuries, and an “autonomous republic” in the Soviet Union and later the Russian Federation. For decades, Moscow administered Chechnya as a unit with Ingushetia, which lies to the west. By contrast, Georgia, to the south, has enjoyed full independence since the breakup of the Soviet Union at the end of 1991.

Ethnic Chechens, as well as the Ingush minority in Chechnya, are Muslim, and their shared religion has long been a rallying point for resistance against Russian rule. In 1791, their Sheikh Mansur, a national hero and symbol of Chechen resistance, lost a key battle to the Russians, yet Russia did not truly secure control for several more decades. In the 1830s, Muslim leader Shamil prosecuted a campaign of guerrilla warfare against the Russians, and when the latter were diverted by the Crimean War in the 1850s, it seemed that the Chechens might successfully break away. As soon as Russia turned its attention to the Chechen problem, however, it crushed Shamil’s revolt.

In 1917, the new Bolshevik government created a joint Chechen and Ingush entity that would eventually be given the name “Chechen Ingush Autonomous Region.” During World War II, Soviet dictator Josef Stalin used alleged Nazi sympathies on the part of the local populace as a pretext for a mass deportation in 1944. Thousands of Chechens and Ingush died in transit, or as a result of deliberate Soviet actions. Only in 1957 were they allowed to return to their homeland, where they remained an obscure fringe element of the Soviet empire until that empire began to crumble.

**The first Chechen war (1991–96).** In August 1991, Chechen politician and former Soviet air force general Dzhokhar Dudayev led a coup against the local Moscow-appointed government. Elected president on October 27, he declared independence on November 1. In 1992, Checheno-Ingushetia split in two, with Dudayev still leading the Chechen portion, and in 1993, he dissolved Chechnya’s parliament.

Over the course of 1994, Moscow attempted to foment a coup by backing anti-Dudayev groups within Chechnya. When these efforts failed to yield fruit, President Boris Yeltsin in November ordered the Chechens to peaceably accept Russian sovereignty or face armed intervention. When the Chechens did not surrender the reins of

government, Russia invaded with a force of 40,000 men on December 11, 1994.

In a situation that recalled the Soviet debacle in Afghanistan that had begun almost exactly 15 years earlier, the Russians found themselves thwarted in their hopes for easy victory. Pushed back from the capital city of Grozny, they only managed to take it in March 1995, at a heavy military and civilian cost. In April, Yeltsin ordered a unilateral ceasefire, but sporadic fighting continued throughout the spring. Only in June did peace talks begin.

January 1996 saw a Russian incursion in neighboring Dagestan, where rebels had seized control of a hospital. Meanwhile, fighting went on as before in Chechnya, and though Yeltsin on March 31, called for a limited withdrawal, this did nothing to abate hostilities. Anti-Russian sentiment in Chechnya flared when a rocket attack killed Dudayev on April 21, and on August 6, rebel forces gained control of Grozny. Then, on August 31, newly instated Russian security chief Alexander Lebed signed a pact with the rebels, declaring the war concluded and putting off the question of Chechen independence.

**The second Chechen war (1997–99).** In 1997, Aslan Maskhadov, leader of one of the anti-Dudayev forces, was elected president of Chechnya. That May, Maskhadov and Yeltsin signed a peace treaty, but still failed to address the question of Chechnya's future status. Resentment of Russian rule continued, and with it sporadic armed resistance.

August 1999 saw more incursions into Dagestan, this time on the part of Chechen rebels, who seized control of several towns. Meanwhile, Russia, which had sponsored terrorist movements worldwide during the Soviet years, for now became the target of terrorism as Chechen separatists set off a wave of bombings in Russia proper. Chechen separatists destroyed four apartment buildings in Moscow, and by the end of September, more than 300 people had died in terrorist incidents across the country.

Although the Kremlin had opposed the U.S. and allied European bombing of Yugoslavia under the aegis of NATO (North Atlantic Treaty Organization) earlier in 1999, in September, the Russians in Grozny emulated the NATO strategy of strategic air offensives. At month's end, however, it became clear that bombing alone would not be enough, and as midnight approached on September 30, several thousand Russian soldiers, with the support of some 1,000 armored vehicles, advanced into northern Chechnya.

At the end of October came an announcement from Russia's defense minister, Igor Sergeev, that Russian troops would remain in Chechnya "for a long time and seriously." This marked a reversal of Moscow's claim, made at the beginning of the offensive, that it was acting only to stop Chechen incursions into Dagestan. Meanwhile, the Russians had set up a government under the leadership of a pro-Russian parliament whose members had been living in Moscow since 1996.

**Chechnya since 1999.** By the end of the 1990s, it was estimated that some 100,000 people had died, and more than 400,000 were rendered homeless, by the wars in Chechnya. In 2002, actions by Chechen troops and terrorists against the Russians continued, with suicide bombings, the downing of a Russian helicopter, and—most dramatically—the storming of a Moscow concert hall in late October. The Russian government responded to the terrorists by gassing the building, rescuing most of the hostages, while killing some hostages along with the perpetrators.

On November 3, 2002, Sergei Ivanov, who had replaced Sergeev as defense minister, announced that Russia would intensify military operations in Chechnya. Military activity continued, but in early 2003, Russia signaled a new strategy. It declared six months' amnesty for all who had fought on either side in the Chechen conflict since 1993, offering all combatants—including convicts and those under investigation, though not persons accused of major crimes such as murder—immunity from prosecution or prison time.

The Russian and Chechen governments held a referendum in April, 2003, that saw large voter acceptance for a new Russian-backed constitution. Critics in Chechnya, however, charged that the referendum and constitution were simply a means toward providing an illusion of self-rule. Internationally, leaders of human rights groups, as well as some Western officials, described the election as an attempt by the Kremlin to avoid negotiation with guerrilla forces.

#### ■ FURTHER READING:

##### BOOKS:

Gall, Carlotta, and Thomas De Waal. *Chechnya: Calamity in the Caucasus*. New York: New York University Press, 1998.

Knezy, Stasys, and Romanas Sedlickas. *The War in Chechnya*. College Station: Texas A&M University Press, 1999.

Lieven, Anatol. *Chechnya: Tombstone of Russian Power*. New Haven, CT: Yale University Press, 1998.

Politkovskaia, Anna. *A Dirty War: A Russian Reporter in Chechnya*. London: Harvill, 2001.

##### ELECTRONIC:

Chechnya News. <<http://www.chechnyanews.com/>> (April 30, 2003).

Pravda. <<http://english.pravda.ru/>> (April 30, 2003).

Russian Informational Centre. Ministry for Press, Television, Radio Broadcasting and Mass Communications of the Russian Federation. <[http://www.infocentre.ru/eng\\_user/](http://www.infocentre.ru/eng_user/)> (April 30, 2003).

##### SEE ALSO

*Cold War (1972–1989): The Collapse of the Soviet Union*



*Kosovo, NATO Intervention  
Russia, Intelligence and Security*

## Chemical and Biological Defense Information Analysis Center (CBIAC)

### ■ JUDSON KNIGHT

The Chemical and Biological Defense Information Analysis Center (CBIAC) is a civilian-operated institution that contracts with the United States Department of Defense (DOD) to provide information on chemical and biological warfare technology. Headquartered in Maryland, it has satellites throughout the United States. CBIAC is a full-service DOD information analysis center operated by Battelle Memorial Institute, and supported by a number of other technology and information entities in the private sector.

CBIAC's mission is to generate, acquire, process, analyze, and disseminate information on chemical and biological (CB) science and technology. It operates under contract to the Secretary of Defense, and is managed by the Defense Technical Information Center under the information analysis center (IAC) program. The information it produces is intended to support commanders, warfighters, and reservists; the CB defense research, development, and acquisition community; and various federal, state, and local departments and agencies in need of current CB information.

**CBIAC operations.** The Defense Department established CBIAC in 1986, and placed Battelle Memorial Institute in charge of its operations. Founded in Columbus, Ohio, in 1929, Battelle is an information and technology company involved in a wide array of disciplines. Among the most notable examples of its achievements are the office copier machine, bar code symbol, and compact disc, all of which are the direct or indirect result of Battelle research and development.

Working with Battelle specialists at CBIAC headquarters in Aberdeen Proving Ground, Maryland, are representatives of Horne Engineering Services, Innovative Emergency Management, MTS Technologies, Quick-Silver Analytics, and SciTech. Together they assist DOD and other government agencies, as well as approved contractors, with the use of CB information for integrated solutions. In addition to its headquarters, CBIAC maintains satellite operations in Arlington and Stafford, Virginia;

Natick, Massachusetts; Saint Robert, Missouri; San Antonio, Texas; and Dugway Proving Ground, Utah.

**Activities of CBIAC.** In accordance with its responsibilities to the DOD, CBIAC identifies and acquires CB data and information from media sources; processes, stores, and retrieves CB data and information; identifies, develops, and applies tools and techniques for the analysis, interpretation, and application of such data and information; and prepares reports, tables, and other forms of focused information for military field personnel, managers, planners, scientists, and engineers.

Among the areas of interest for CBIAC are analysis of manufacturing processes for nuclear, biological, and chemical (NBC) systems; identification of chemicals and the physical and chemical properties of chemical warfare/chemical and biological defense (CW/CBD) materials; combat effectiveness; counter-proliferation, international technology proliferation, and arms control; counter-terrorism; decontamination; demilitarization, conversion of CB materials and equipment for defense purposes, and technology transfer for dual use; individual and collective protection and domestic preparedness; environmental effects of CB materials; force protection; and many others.

CBIAC attempts to anticipate the requirements for CB information, and seeks to work with emerging CB defense organizations. Its products range from handbooks and training kits to computerized databases, interactive software, and CD ROMs. Additionally, it offers inquiry and referral services whereby it provides answers and information relevant to specific CB needs. CBIAC also maintains an extensive library, containing some 108,000 citations of CB information, as well as 41,000 holdings.

### ■ FURTHER READING:

#### BOOKS:

- Drell, Sidney D., et al. *The New Terror: Facing the Threat of Biological and Chemical Weapons*. Stanford, CA: Hoover Institution Press, 1999.
- Joseph, Robert G., and John F. Reichart. *Deterrence and Defense in a Nuclear, Biological, and Chemical Environment*. Washington, D.C.: Center for Counterproliferation Research, National Defense University, 1999.

#### ELECTRONIC:

- Battelle Memorial Institute. Defense Systems—CBIAC. <<http://www.battelle.org/army/cbiac.stm>> (January 17, 2003).
- Chemical and Biological Information Analysis Center. <<http://www.cbiac.apgea.army.mil/>> (January 17, 2003).

#### SEE ALSO

*Biochemical Assassination Weapons*  
*Biological Warfare*  
*Chemical Warfare*



A technician collects a sample from a laptop computer that will be analyzed by the Sabre 2000 trace detection instrument, which can detect traces of explosives, drugs, or chemical weapons. AP/WIDE WORLD PHOTOS.

## Chemical and Biological Detection Technologies

■ BRIAN HOYLE

The ability to detect the components of chemical and biological weapons is an important part of a national security strategy. For example, the inability to rapidly detect letters for the presence of anthrax spores provided a route for the targeting of infectious microorganisms in the United States in 2001. The portability of chemical and biological weapons has made them attractive to individuals or groups with political, religious, or other grievances. This has spurred development of more sophisticated, accurate and rapid detection technologies.

The conventional x-ray technology long used in airports has been refined. Most of the x-ray beam is reflected back immediately upon encountering an object. Some of the radiation, however, passes through the object. By analyzing the beams that actually penetrate through an

object, information on the object's composition is provided. Another version sends two different x rays of different wavelengths through an object. The different beams can distinguish between organic objects, such as food and paper, and inorganic objects.

A chemical detection technology known as gas chromatography has been sped into routine use in airports since the U.S. terrorist attacks of September 11, 2001. The different chemicals present on a cloth that is swiped over an object can be separated based on their different preference for the gas mixture that is pumped through the sample chamber. A target chemical (i.e., an explosive) is detected within seconds.

Chemical detection technologies have also been adapted for use "in the field", such as by United Nations inspectors deployed in Iraq beginning in November 2002, to the presence of missiles that were supposedly destroyed by the Iraqi government in the mid-1990s.

Sound can be used to detect chemicals. For example, the acoustic wave sensor uses a quartz surface to convert incoming sound waves into electrical signals. Over a dozen different chemicals can be detected within seconds, even from biological sources. In another sound-based technique called acoustic resonance, the pattern of vibrations when sound waves are sent inside an object like a missile can reveal whether the missile is filled with a solid or a liquid, and even the type of chemical present.

Light is another means of chemical detection. The use of light is called spectroscopy. Mass spectroscopy determines the mass of proteins, which is important in determining the identity of the chemical or biological agent. Matrix-Assisted Laser Desorption/Ionization Mass Spectroscopy (MALDI-MS) can identify proteins that are unique to *Bacillus anthracis* (the cause of anthrax) and *Yersinia pestis* (the cause of plague). Raman spectroscopy measures the change in the wavelength of a light beam by the sample molecules. Optical spectroscopy measures the absorption of light by the chemical groups and the subsequent emission of light by the same groups as the identification method.

The ability to detect genetic sequences that are unique to certain bacteria (gene probing) has been exploited to develop genetically based microbial detection methods. The best example of gene probing is the polymerase chain reaction (PCR), which can enzymatically detect a target stretch of genetic material and rapidly amplify that region to detectable levels. Handheld PCR detectors (i.e., Handheld Advanced Nucleic Acid Analyzer, or HANAA) were used in the 2002–2003 inspections of Iraqi facilities by United Nations officials.

Biological detection devices can monitor the surrounding air at regular intervals. Air is automatically drawn into the device and analyzed for target genetic sequences using the PCR technology. The results can be electronically relayed to a central base for analysis.

Another biological technology utilizes antibodies that are produced in response to the presence of a specific

microorganism. Tests are available that detect *Bacillus anthracis*, *Clostridium botulinum*, viruses (e.g., smallpox), and chemicals (e.g., ricin) in minutes.

Some older biological detection technologies still prove reliable. Growth of microorganisms on artificial food sources (media) produces populations called colonies. Medium can be selected that produces colonies that have a distinctive appearance and color. Gel electrophoresis separates differently sized pieces of genetic material or other microbial components (e.g., protein) into bands. The banding pattern can be used to identify the microorganism. Finally, chromatography separates compounds from one another based on their differing speed of movement through a gas or a liquid mixture.

#### ■ FURTHER READING:

#### BOOKS:

Cilluffo, Frank J., Sharon L. Cardash, and Gordon Nathaniel Lederman. *Combating Chemical, Biological, Radiological, and Nuclear Technologies: A Comprehensive Strategy: A Report of the Csis Homeland Defense Project*. Washington, D.C.: Center for Strategic and International Studies, 2001.

Fritz, Sandy, and Jack Brown. *Understanding Germ Warfare (Science Made Accessible)*. New York: Warner Books, 2002.

Lederberg, Joshua, and William S. Cohen. *Biological Weapons: Limiting the Threat (BCSIA Studies in International Security)*. Boston: MIT Press, 1999.

United States Department of Defense. *21st Century Bioterrorism and Germ Weapons: U.S. Army Field Manual for the Treatment of Biological Warfare Agent Casualties (Anthrax, Smallpox, Plague, Viral Fevers, Toxins, Delivery Methods, Detection, Symptoms, Treatment, Equipment)*. Washington, D.C.: Progressive Management, 2001.

#### SEE ALSO

*Air Plume and Chemical Analysis*  
*Biocontainment Laboratories*  
*Bomb Detection Devices*

## Chemical and Biological Mass Spectrometer (CBMS).

SEE *Oak Ridge National Laboratory (ORNL)*.

## Chemical Biological Incident Response Force, United States

■ JUDSON KNIGHT

The Chemical and Biological Incident Response Force (CBIRF) is a unit of the United States Marines devoted to countering chemical or biological threats at home and abroad. Activated in 1996, the unit served a number of protective functions. Since the terrorist bombings of September 11, 2001, however, its prominence has increased dramatically. Now part of the 4th Marine Expeditionary Brigade (MEB), it has performed homeland security functions that included the removal of suspected toxic agents from House and Senate office buildings during a rash of anthrax attacks in late 2001.

### Background and Mission

Chemical agents have been a widespread threat since World War I, when first used by German forces on the Eastern Front in 1915. Soon the British developed their own chemical weapons, and the age of chemical warfare began, forever altering the battlefield equation. Use of chemical weapons by Saddam Hussein on Kurdish civilians, use by both Iran and Iraq during their prolonged war in the 1980s, and use during the 1994 and 1995 attacks by Aum Shinrikyo (a Japanese cult) that released deadly sarin gas into the Tokyo subways and killed 12 civilians, demonstrate that both military and civilian personnel are increasingly vulnerable to chemical attacks.

On June 21, 1995, partly in response to the Aum Shinrikyo attacks, as well as the Oklahoma City bombing on April 19 of that year, the administration of President William Jefferson Clinton issued Presidential Decision Directive 39, "United States Policy on Counterterrorism." The directive called for a number of specific efforts to deter terrorism on America's shores, as well as that against Americans and allies abroad. In response to the need for a response team to deal with chemical and biological threats, the United States Marine Corps established CBIRF (the first two words are sometimes rendered as "Chemical Biological" or "Chemical, Biological) on April 4, 1996.

**Training exercises.** Writing in the Marine Corps magazine *Leatherneck*, Margaret Bone described CBIRF thus in early 1999: "It's new, it's unique to the Armed Services, and right now, it's the only quick reaction force in the world equipped to help in the aftermath of a chemical, biological, or radiological (nuclear) attack." But the writer went

on to note that “CBIRF is not a counterterrorist group, and it’s not direct-action oriented, though there is a security element of more than 120 Marines, with the capability to increase that strength as needed.” In the words of a force protection element commander for CBIRF, “We are a consequence management force. Our mission is to respond, to come in and save lives. We bring the full package: self-contained, expeditionary, and task-organized.”

During the spring and early summer of 1996, CBIRF was deployed for training in a variety of environments throughout the United States. Its members closely studied the bombing that took place at Centennial Olympic Park in Atlanta on the night of July 27, and practiced coordinating a response with local fire and police. They also undertook an experiment at the Citadel, a military college in Charleston, South Carolina, where CBIRF personnel acted to control lethal agents released by a mock chemical weapons plant. Moving beyond training to real-world situations, CBIRF provided security for President Clinton’s second inauguration in January 1997, and for the Summit of Eight in Denver, Colorado, that following summer.

**A changing role.** In the aftermath of the September 11, 2001, terrorist attacks on the United States, CBIRF’s mission became incorporated into the 4th MEB, along with the Marine Security Force Battalion, the Marine Security Guard Battalion, and the new anti-terrorism battalion. (The latter had evolved from the 1st Battalion, 8th Marines, which had been hit in the 1983 terrorist bombings of United States Marine barracks in Lebanon.) In December 2001, CBIRF sent a 100-member initial response team into the Dirksen Senate Office Building alongside Environmental Protection Agency (EPA) specialists to detect and remove anthrax. A similar mission was undertaken at the Longworth House Office Building in October, during which time samples were collected from more than 200 office spaces.

#### ■ FURTHER READING:

##### PERIODICALS:

- Bone, Margaret. “Marines Provide Safety Net to Terrorist Threat.” *Leatherneck* 82, no. 2 (February 1999): 50–53.
- Cabellon, Paul C. “CBIRF Takes the (Capitol) Hill.” *Leatherneck* 85, no. 2 (February 2002): 19.
- Garamone, Jim. “Marines to Stand up Anti-Terror Brigade.” *Pentagon Brief* (October 2001): 5.
- Vogel, Steve. “Cooler Name Prevails for ‘Hot’ New Marine Corps Club at Indian Head.” *Washington Post*. (April 26, 2001): T15.

##### SEE ALSO

*Chemical Safety: Emergency Responses*  
*Chemical Warfare*

## Chemical Safety and Hazard Investigation Board (USCSB), United States

■ CARYN E. NEUMANN

The United States Chemical Safety and Hazard Investigations Board (USCSB) is a federal agency formed to identify the causes of chemical accidents. Created in 1990 as part of an amendment to the Clean Air Act, the USCSB did not begin functioning until it received funding in 1998. Although its purpose overlaps that of other federal agencies, notably the Occupational Safety and Health Administration (OSHA), the Environmental Protection Agency (EPA), and the National Transportation Safety Board (NTSB), the USCSB differs from these organizations in that it does not have the power to make or enforce rules affecting the routine day-to-day activities of businesses. Instead, the USCSB makes a unique contribution to the protection of workers, the public, and the environment by investigating chemical accidents in the country and attempting to prevent future mishaps. The only regulations put into place by the fact-finding agency involve the reporting of chemical incidences.

The establishment of the Washington, D.C.-based USCSB is a result of the belief that existing hazard investigation agencies, like OSHA, EPA, and NTSB, focus on violations of existing rules while ignoring factors that contribute to a chemical accident, but which do not constitute a violation of existing rules and regulations. By creating this independent, scientific, investigatory agency and modeling it after the NTSB, Congress hoped to produce fuller accident reports that could then be used to formulate new regulations and policies to prevent future dangerous chemical spills and explosions. The amended Clean Air Act of 1990 that gave birth to the USCSB directs the board to investigate and report on the circumstances and the probable causes of chemical incidents resulting in a fatality, serious injury, or substantial property damages; recommend measures to reduce the likelihood or the consequences of such accidents and propose corrective measures; and, lastly, to establish regulations for reporting accidental releases. The board has no enforcement authority, does not issue fines or penalties, and essentially plays a very limited regulatory role.

Accidental releases of toxic and hazardous chemicals occur frequently and often have serious consequences. The USCSB is notified of every chemical release in the country and then decides which accidents to investigate. It is required to coordinate its activities with OSHA, NTSB, and EPA, but when an accident involves transportation, NTSB is the lead agency. Board members, appointed by the president to five-year renewable terms and confirmed by the Senate, are ultimately responsible for the conduct of investigations and the content of accident reports.

## Chemical Safety: Emergency Responses

■ JUDSON KNIGHT

Staffers and contractors conduct the actual investigations, which typically involve extensive site visits, evidence collection, and analytical work. Investigators may issue brief summary or detailed investigative reports. Some investigations may conclude without the issuance of any report. Accident reports must be approved by a majority vote of the five board members before they are issued. As of 2000, the USCSB had issued only a handful of reports, in part because of insufficient staffing but also as a result of serious disagreements among board members. Staff levels have since been raised and the board has established a more harmonious working arrangement. The agency is in the process of developing the Chemical Incidents Reports Center, an online database of chemical incidents that have occurred worldwide, in the hopes that the site may inspire researchers to investigate the incidents that the USCSB cannot examine for lack of resources.

The rise in global terrorism and the corresponding fear of a terrorist attack that utilizes chemicals makes the USCSB an important component of American homeland security. By identifying hazardous practices, the agency promotes preventive actions by the public and private sectors that may make it more difficult for terrorists to create chemical incidents.

### ■ FURTHER READING:

#### BOOKS:

United States General Accounting Office. *Chemical Safety Board: Improved Policies and Additional Oversight Are Needed*. Washington, D.C.: GPO, 2000.

———. *Chemical Safety Board: Realigned Management Faces Serious Challenges: Testimony Before the Subcommittee on Veterans Affairs, Housing and Urban Development, and Independent Agencies, Committee on Appropriations, U.S. Senate*. Washington, D.C.: GPO, 2000.

#### ELECTRONIC:

United States Chemical Safety and Hazard Investigation Board. "Chemsafety.gov." <<http://www.chemsafety.gov/about>> (January 19, 2003).

#### SEE ALSO

*Chemical Safety: Emergency Responses*  
*Chemical Warfare*  
*Chemistry: Applications in Espionage, Intelligence, and Security Issues*  
*NTSB (National Transportation Safety Board)*

When the United States as a whole, or any portion or property of the federal or state governments, is threatened by a chemical hazard, a host of agencies go into action. Communities, neighborhoods, and localities are also encouraged—and in some cases required—to develop their own emergency response plans. In the event of a chemical threat, communities are protected by provisions in the Emergency Planning and Community Right-to-Know Act (EPCRA). Passed by Congress in 1986, EPCRA establishes guidelines whereby federal agencies assist local communities in the event of a toxic chemical spill or related incident. EPCRA also provides a framework for action both by citizens and state governments.

There are numerous federal offices assigned to handle threats involving the release, whether intentional or accidental, of hazardous chemicals. Most notable among these is the Coast Guard National Response Center, the first point of contact for information on hazardous-waste spills and a host of other threats to the environment or infrastructure. Within the Department of Defense, the U.S. Army and Marines both have forces designed to respond to chemical threats, as do a number of other departments of the federal government. Likewise, Washington oversees civilian-run installations, such as the Atmospheric Release Advisory Capability, to monitor chemical and other threats. These and other agencies are discussed elsewhere; in the present context, the primary concern is the local, civilian response to chemical hazards.

**EPCRA provides a response plan.** Motivated by concerns raised by the disaster in Bhopal, India, where in 1984 some 2,000 people lost their lives due to an accidental release of toxic chemicals, Congress passed EPCRA. The latter established requirements for federal, state, and local governments, Indian tribes, as well as for industry, with regard to emergency planning and "community right-to-know" concerning toxic chemicals. In addition to emergency planning and emergency release notification, EPCRA addresses hazardous chemical storage reporting requirements and toxic chemical release inventories.

Under the provisions of EPCRA, each state governor appoints a state emergency response commission (SERC). The SERCs have in turn designated a total of about 3,500 local emergency planning districts nationwide. For each of these, the SERC appoints a local emergency planning committee (LEPC). Under the guidance of the SERC, the LEPC develops a community emergency response plan



A chemical, biological incidence response force (CBIRF) responds to a mock emergency at the Defense Language Institute in Monterey, California. AP/WIDE WORLD PHOTOS.

designed to identify threats, establish workable emergency procedures, assess preparedness, train local response teams, and take steps to maintain supplies and schedules in preparation for any possible threat.

**Federal assistance.** In the event of a terrorist attack involving hazardous chemicals, guideline provisions direct that local authorities should establish an incident command system that may eventually become a unified command involving federal authorities. Under such circumstances, the Federal Bureau of Investigation is usually designated the lead federal agency. Meanwhile, the Federal Emergency Management Agency acts as the lead office for coordination of federal support to state and local personnel. Also involved are the National Response Team, Environmental Protection Agency (EPA), Department of Health and Human Services, and Department of Defense.

In accordance with the federal response plan, a national contingency plan for response to disasters, federal agencies are grouped into one of 12 functional areas for emergency support functions (ESFs). For example, EPA, which is heavily involved in oversight regarding EPCRA compliance and preparedness, falls under ESF 10, Hazardous Materials. EPA personnel work to determine the nature of the hazardous substance released, and follow up

with environmental monitoring, decontamination, and long-term cleanup of the affected site.

#### ■ FURTHER READING:

##### BOOKS:

*The EPCRA Compliance Manual: Interpreting and Implementing the Emergency Planning and Community Right-to-Know Act of 1986.* Chicago: American Bar Association Section of Environment, Energy, and Resources, 1997.

*EPCRA: Emergency Planning and Community Right-to-Know Act.* Chicago: American Bar Association Section of Environment, Energy, and Resources, 2002.

*EPCRA Section 313 Questions and Answers: Section 313 of the Emergency Planning and Community Right-to-Know Act, Toxic Chemical Release Inventory.* Washington, D.C.: United States Environmental Protection Agency Office of Pollution Prevention and Toxics, 1999.

##### ELECTRONIC:

RCRA, Superfund, and EPCRA Call Center. <<http://www.epa.gov/epaoswer/hotline/>> (January 29, 2003).

##### SEE ALSO

*Coast Guard National Response Center*



Hazardous material response team members don protective gear during an exercise designed to train for an emergency involving chemical weapons stored in the U.S. Army arsenal at Pine Bluff, Arkansas. AP/WIDE WORLD PHOTOS.

*Homeland Security, United States Department  
United States, Counter-Terrorism Policy*

---

## Chemical Warfare

---

■ BRIAN HOYLE

Chemical warfare involves the aggressive use of bulk chemicals that cause death or grave injury. These chemicals are different from the lethal chemical compounds that are part of infectious bacteria or viruses. The latter constitute biological warfare.

### History of Chemical Warfare

The use of chemicals in warfare began centuries ago, when early combatants learned that smoke from burning sulfur caused discomfort when it drifted into enemy fortifications. The dawn of modern chemical warfare occurred

during World War I. On April 15, 1915, German forces released about 160 tons of chlorine gas into the wind near the Belgian village of Ypres. The clouds of the gas drifted into Allied forces, killing some 5,000 soldiers. Two days later, another chlorine attack at the same village killed 5,000 more soldiers.

During the remainder of World War I, German and British forces used chlorine gas, and other chemicals (i.e., mustard gas and phosphene) with increasing tendency. Estimates are that approximately 113,000 tons of chemical weapons were used from 1915 to 1918, killing some 92,000 people and injuring over one million people.

The aerial release of chemicals brought unpredictable results at the mercy of prevailing winds. Shifting winds could send the deadly cloud back to the attacking troops. Later during World War I, more sophisticated use of chemical weapons began. For example, the French used shells filled with an irritant to the eyes, skin, and lining of the nose and lungs, and the Germans fired lead balls coated with similar irritant.

The horrors of chemical warfare during World War I prompted the drafting of the Geneva Protocol of 1925, which banned chemical and biological weapons of warfare. The protocol was initially signed by 38 nations (now over 130 nations). As history has shown, the protocol has



Terrified children run from their village after a U.S. napalm attack during the Vietnamese War. This photograph was pivotal in promoting awareness of the suffering of the Vietnamese people during the war and was particularly effective in arguments against the use of napalm. AP/WIDE WORLD PHOTOS.

not stopped the use of such weapons by rouge states or fringe elements in order to commit terrorism.

Aerial releases of lethal chemicals did not occur in World War II. However, the Germans developed a new class of chemical weapon called nerve agents. During the 1930s and 1940s, agents such as Tabun, Sarin, and Soman were created.

Chemical warfare research continued during the Cold War tensions during the 1950s. During this time, military chemists in the United Kingdom and then in the United States adapted insecticides to produce the most lethal chemical agent then known. The agent was code named VX. The potency of VX was accidentally demonstrated in 1968, when a testing accident at the VX manufacturing plant in Dugway, Utah killed over 6,000 sheep.

During the Vietnam War of the 1970s, the U.S. use of defoliants—chemicals that killed vegetation, permitting a clearer detection of the enemy—was extensive. One of these compounds, Agent Orange, has become infamous

as the alleged cause of a variety of physical ailments in veterans of the conflict.

In the last few decades, chemicals have become the tools of terrorists. A particularly well-known example is the release of Sarin gas into the Tokyo subway system by the religious cult Aum Shinrikyo in March of 1995. The gas killed 12 people and injured over 5,500 people in 16 stations.

## Chemical Warfare Agents

There are several classes of chemical warfare agents, based on their effects:

- compounds that cause choking or that irritate the lungs,
- blister agents (also called vesicants),
- blood agents,
- nerve agents,
- herbicides, and





A member of a biological and chemical warfare response team wearing a protective suit carries a suspicious envelope in a bag at Jerusalem's Malcha shopping mall in 2001. AP/WIDE WORLD PHOTOS.

#### ■ incendiaries

**Choking and irritant agents.** There are a number of compounds that cause choking or irritation of lung tissue. Examples include chlorine, phosgene (carbonyl chloride), diphosgene, chloropicrin, ethyldichloroarsine, and perfluroisobutylene.

Chlorine gas is suffocating and quickly burns tissues in the nose, mouth, and lungs. The burned tissue can die and slough off, causing lasting damage. Chlorine gas dissipates in the air very quickly. If exposure is not too long, than damage can be minor. In contrast, the compound called disphosgene is a liquid at room temperature, and so persists much longer.

**Blister agents.** As their name implies, blister agents cause the formation of large and painful blisters on the skin. Eye and lung tissue can also be damaged. A well-known example of a blistering agent dating from World War I is mustard gas. The damage to cells of the skin cause blistering up to 24 hours after exposure to mustard gas. These

blisters take a long time to heal and can send the body into a lethal shock reaction.

Other examples of blistering agents include nitrogen mustard, lewisite, and phenyldichloroarsine. The latter compound is a liquid, which can be sprayed onto an enemy or released from a balloon, helicopter, or airplane.

**Blood agents.** These compounds interfere with the body's ability to transport oxygen in the bloodstream. This is done by either blocking the use of oxygen by cells in the body or by blocking the ability of the blood to take up the oxygen. Examples include hydrogen cyanide (also called prussic acid), cyanogen chloride, arsine, carbon monoxide, and hydrogen sulfide.

Hydrogen cyanide is initially a liquid at room temperature, but it quickly evaporates. This compound is noteworthy in recent world history, as it was used by Iraq in 1988 on an attack on the Kurdish town of Halabja during the Iran-Iraq war. Because of its past use by Iraq, hydrogen cyanide was one of the major concerns of United Nations inspectors who inspected various facilities in Iraq during the winter of 2003.

Compounds such as arsine and carbon monoxide destroy the ability of the hemoglobin component of the blood to bind oxygen. Arsine does this by destroying the red blood cells. Carbon monoxide binds to hemoglobin, blocking the binding of oxygen.

**Nerve agents.** Compounds that are classified as nerve agents interfere with the body's transmission of nerve impulses. This is done by disrupting the activity of a chemical called acetyl cholinesterase, which functions to bridge the gap between adjacent nerve cells, permitting an electrical nerve signal to pass from one nerve cell to the next.

Nerve agents were first developed in 1936, following the development of organophosphate types of pesticides. The first nerve agent that was made is called Tabrun. It is a member of what is known as the G series of nerve agents. Other G series members are Sarin and Soman. Sarin is particularly lethal; a small amount absorbed through the skin can kill a man within two minutes. When inhaled, death occurs within 15 minutes. Sarin is infamous as the gas released into the Tokyo subway system by the fringe group Aum Shinrikyo in 1995.

Another series of nerve agents are called the V series. Members of this series—which are commonly abbreviated according to their chemical composition—are more potent than the agents of the G series. As well, they persist longer in the environment. They can, for example, be applied to surfaces like roads as a slime.

Examples of V series agents include VX, VE, VG, and VM. VX is extremely potent; a drop of the liquid absorbed through the skin is lethal within a few hours without treatment.

Nerve agents can be contained in missiles or in canisters for lengthy time periods. Examination of caves in Afghanistan that were used as strongholds by the terrorist group al Qaeda has revealed evidence of stores of Sarin and VX.

**Herbicides.** Herbicides are chemicals that kill vegetation. Such chemicals are often used in everyday life to keep lawns free of weeds (although more environmentally-friendly alternatives are becoming popular). When used in war, herbicides are weapons of mass destruction to foliage. Destruction of plants and the resulting loss of leaf cover remove much of the concealment for an enemy in a forested area. These philosophies led to the massive use of Agent Orange by the United States in the Vietnam War in the 1970s. Since that war, the damaging effects of herbicides like Agent Orange and paraquat on the human nervous and immune systems has become evident.

**Incendiaries.** Incendiaries are chemicals that cause fires. In warfare, they are also to remove vegetation. An infamous incendiary is napalm. Napalm is a mixture of naphthenic acid, coconut fatty acids, and palm oil. In addition to its highly flammable property, napalm absorbs into exposed skin, where it can cause severe burns if ignited. Napalm was used as an offensive weapon by the United States during the Vietnam War.

## Modern Day Chemical Warfare

In 2003, the use of chemical weapons remains a threat from rogue states and terrorists. Current world attention is focused on the former chemical warfare capabilities of Iraq. It is known that Iraq engaged in chemical warfare research and weaponization in the 1980s and 1990s, and as of early 2003, before the U.S. war in Iraq, had not fully complied with United Nations resolutions requiring disclosure and destruction of their chemical weapons program.

### ■ FURTHER READING:

#### BOOKS:

- Ellison, D. Hank. *Handbook of Chemical and Biological Warfare Agents*. Boca Raton: CRC Press, 1999.
- Harris, Robert, and Jeremy Paxman. *A Higher Form of Killing: The Secret History of Chemical and Biological Warfare*. New York: Random House, 2002.

#### PERIODICALS:

- Macintyre, A. G., C. G. W. Eitzen, Jr., R. Gum, et al. "Weapons of Mass Destruction Events with Contaminated Casualties: Effective Planning for Health Care Facilities." *Journal of the American Medical Association* no. 283 (2000): 252–253.
- Munro, N.B., S.S. Talmage, G.D. Griffin, et al. "The Sources, Fate, and Toxicity of Chemical Warfare Agent Degradation Products." *Environmental Health Perspectives* no. 107 (1999): 933–974.

- Nakajima, T., S. Ohta, Y. Fukushima, et al. "Sequelae of Sarin Toxicity at One and Three Years after Exposure in Matsumoto, Japan." *Journal of Epidemiology* no. 9 (1999): 337–343.

#### ELECTRONIC:

- How Stuff Works. "How Biological and Chemical Warfare Works." 2002. <<http://www.howstuffworks.com/Biochem-war.htm>>(10 January 2003).

#### SEE ALSO

- Chemical and Biological Detection Technologies USAMRICD (United States Army Medical Research Institute of Chemical Defense)*

---

# Chemistry: Applications in Espionage, Intelligence, and Security Issues

---

### ■ JUDYTH SASSOON

From the detection of forgeries to the identification of criminal suspects, the techniques of chemistry have many applications in areas relating to espionage, intelligence and security. Analytical chemistry, the branch of chemistry concerned with the analysis of substances, is of particular importance. The study of the chemical composition of a compound gives a qualitative analysis, while the determination if its concentration involves quantitative analysis. Chemists utilize a range of different skills to help security services in areas as wide-ranging as drugs, firearms, toxicology, and fiber analysis. For example forensic chemistry concerns the detection and characterization of substances at crime scenes. These might include bomb fragment analysis, fire investigations, firearms discharge analysis, poison or toxin analysis and various other types of chemical residue analysis. In these instances, sophisticated analytical techniques are used to identify minute residues of paint, fire accelerants, human hair, body fluids or tissues. Advanced spectroscopic and separation procedures can often clarify confusing circumstantial evidence.

Modern analytical chemical laboratories can use both classical "wet" methods (gravimetric or volumetric procedures) employing chemical reactions to perform the analysis, or instrumentation, which makes critical measurements during an analysis. A number of separation methods are useful either prior to chemical analysis or as direct methods in the analysis. These methods include distillation, selective precipitation, filtration, osmosis, and extraction. Most analytical procedures in the forensic laboratory now use some instrumentation and many are fully automated. The instrument-based methods of analysis are divided into categories according to the type of process used to perform the analysis. Optical instruments such



Chemistry students at the National School of Biological Science in Mexico City work with samples of anthrax in October 2001, without customary controls such as biosafety suits and ventilation hoods that are imposed by most other countries. AP/WIDE WORLD PHOTOS.

as spectrosopes comprise the first major group and measure electromagnetic radiation, which is either absorbed (absorption spectroscopy) or emitted (emission spectroscopy) by a sample. The wavelength at which this occurs can be used for qualitative analysis, while the amount of radiation can be useful for quantification. Spectroscopy involves the use of radio, infrared, ultraviolet, visible and x-ray regions of the electromagnetic spectrum.

Of the instrumental separation methods, chromatography and its variations are the most widely used. Chromatography is a technique whereby a mixture is separated into its components by the reactive adherence of each component to a stationary phase while a mobile phase passes over the stationary phase. Chromatography is divided into categories, depending on the physical state of the stationary and mobile phases. Examples include gas-solid, gas-liquid, liquid-liquid or liquid-solid chromatography and also thin layer, paper, and gel permeation chromatography. The applications of these techniques in forensics can provide much intelligence information in the form of physical evidence that can be used subsequently by security forces.

The techniques above are frequently employed in the analysis of substances from sites of criminal or terrorist activity. For example, the examination of debris at the

scene of a fire can provide data to show if the fire started accidentally or deliberately. The correct identification of the source and the presence of accelerants can link the fire to an arson suspect. Similarly, detailed laboratory analysis of debris and trace evidence from explosion scenes (domestic, commercial, suspected criminal, or terrorist) as well as a detailed chemical knowledge of the capacity of materials to form explosions can yield information showing the nature of the source. If a firearm is discharged, gunshot residue such as burnt or partly burnt gunpowder and components from the primer compound (e.g. lead, barium, and antimony) are also thrown out into the surroundings). Firearms discharge residues that may be deposited on any object near to a gun when it is fired, or on any object that subsequently touches the gun. When an object is shot at a relatively close range, gunshot residues are deposited, and sometimes violently impacted, onto the target. The nature and distribution of these residues can match a target to a weapon and can also be used to determine the distance from the gun's muzzle from point of impact.

Chemical analysis becomes important in the study of glass and building materials from the site of an incident. Glass is frequently broken when a criminal offence takes place and building materials such as plaster, mortar, bricks,

slate or loft insulation may be dislodged if illegal entry is gained into a building. Fragments of either can adhere to clothing and may be recovered from a suspect. A comparison of these with similar materials at the incident scene can link a suspect to a crime. Similarly, paint can be conveyed between surfaces following contact, and analysis of paint composition and layering can be used to connect paint fragments to a crime. The most common occurrence is the transfer of paint between vehicles or objects in road traffic accidents. Paint fragments can also adhere to items of clothing following contact with loose flakes on surfaces such as windows at the scene of burglaries. Paint analysis can also be applicable in circumstances where painted car parts are suspected of having been exchanged between vehicles.

Chemical analysis of cloth fibers, stains and organic materials such as human hair and body fluids provide vital evidence in, for example, homicide cases. In the past, biochemical blood typing using antisera and the matching of hair types could not provide absolute identification of a suspect or victim, although it could narrow the possibilities down. Today, however, even minute quantities of blood, semen, skin cells and hair can yield DNA profiles. DNA from different individuals differs in base sequence and, theoretically every individual with the exception of identical twins, can be identified solely on the basis of their DNA sequences. However, a complete DNA analysis of individuals is a daunting and time consuming task because of the many millions of bases in the human genome. The possibilities for routine genome analysis do not exist at present. Instead, DNA matching is performed by analysing shorter, highly polymorphic single locus genes such as the VNTR genes. This method can establish a "DNA signature" for almost any individual. Biochemical analysis of these sequences can determine whether two DNA samples are from the same person, related people, or unrelated people. Though these methods also do not yield absolute certainties, they are nevertheless more precise than traditional methods such as blood typing.

DNA profiling as a crime intelligence aid involves the use of basic chemical and biochemical procedures. DNA is chemically isolated from the cell or tissue sample, amplified using the enzymes in the polymerase chain reaction (PCR), and then analyzed by electrophoretic methods. The DNA profile from the scene of the crime can be compared with a DNA profile from a suspect and a match can link the suspect to the crime. If there is no suspect, the DNA profile can be matched with profiles stored on to the National DNA Database (NDNAD). If there is no match with the NDNAD, it is sometimes decided to carry out an intelligence-led screen (a mass DNA screen). A target group of individuals, for example, men within a certain age range living in a town or area, are asked to voluntarily provide DNA samples, which are then analyzed and compared with a profile linked to a particular crime. Samples from volunteers are not stored on the NDNAD, and are destroyed if they do not match the crime profile.

Thus, the sensitivity and accuracy of chemical analytical methods lie at the heart of forensic science and, with the advances in biochemical techniques, provide essential tools for crime intelligence investigations.

#### ■ FURTHER READING:

##### BOOKS:

Bodziak J., and Jon J. Nordby. *Forensic Science: An Introduction to Scientific and Investigative Techniques*. CRC Press, 2002.

##### PERIODICALS:

Casagrande, R. "Technology against Terror." *Scientific American*. 287 (2002):59–65.

"Early Warning Technology." *Med Device Technol* 13 (2002): 70–2.

##### SEE ALSO

*Biodetectors*  
*Crime Prevention, Intelligence Agencies*  
*Explosive Coal*  
*Forensic Science*  
*Microbiology: Applications to Espionage, Intelligence and Security*  
*Molecular Biology: Application to Espionage, Intelligence and Security Issues*

---

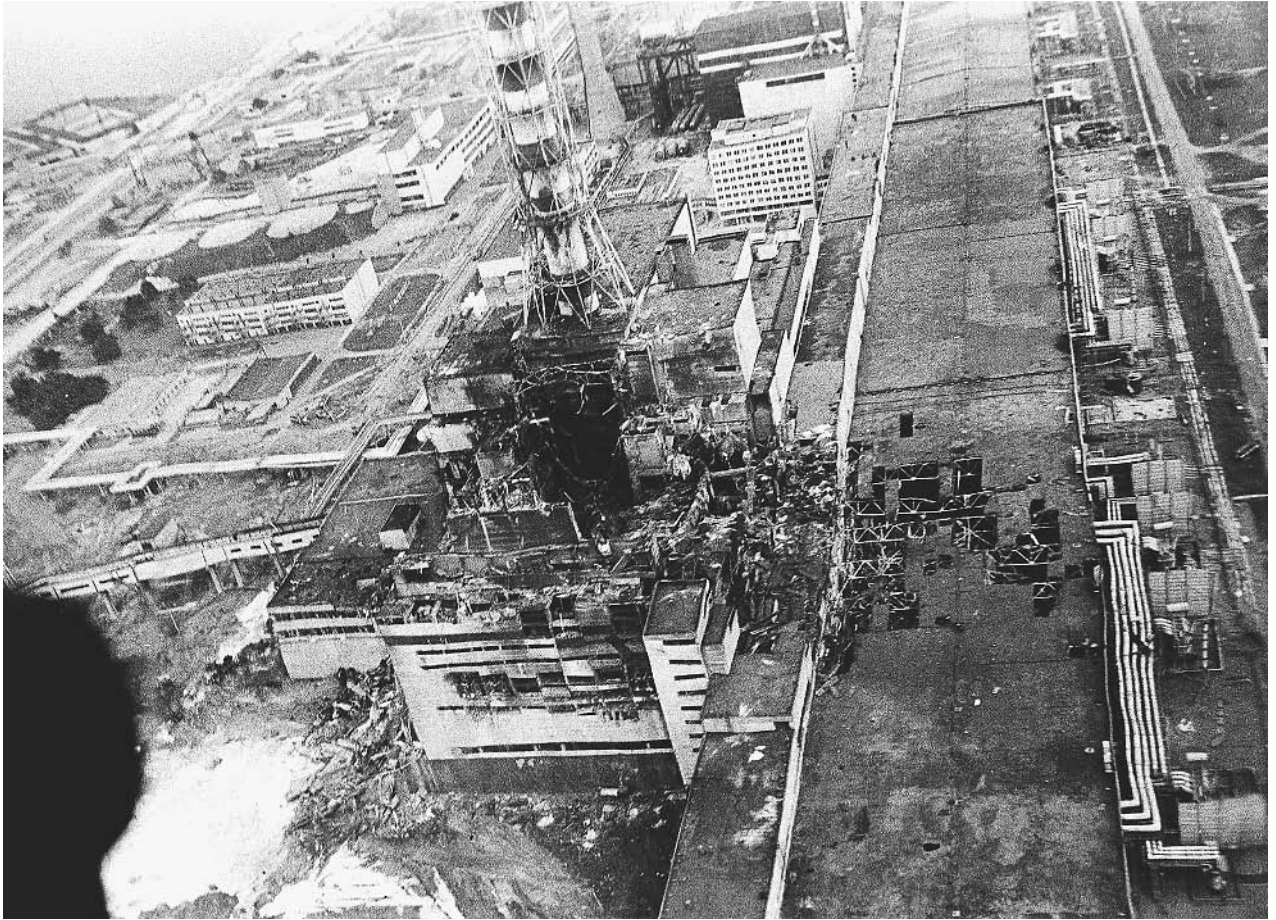
## Chernobyl Nuclear Power Plant Accident, Detection and Monitoring

---

#### ■ LARRY GILMAN

On April 26, 1986, a nuclear reactor in the town of Chernobyl (in the Ukraine, then a member state of the Soviet Union) exploded, collapsing the building in which it was located and releasing a radioactive plume that deposited material over much of Europe and Scandinavia. Although the Soviet government was unwilling to release information, satellite photographs by military and civilian satellites, as well as direct radiation measurements downwind, confirmed the event.

**The accident and its consequences.** The town of Chernobyl, some 60 miles (96 km) north of the city of Kiev (population 2.5 million), is the site of a nuclear electricity-generating station comprising four identical units of the Soviet-designed RBMK1000 type. Each of the four units is designed to produce 1,000 megawatts of electricity; one of the units is still in operation. On April 25, 1986, operators began an experiment at Unit No. 4 to take advantage a scheduled annual maintenance shutdown. The goal of the



An aerial view of the Chernobyl nuclear power plant is shown in this 1986 photo made a few days after the explosion in Chernobyl, Ukraine. AP/WIDE WORLD PHOTOS.

experiment was to see if the station's turbine generator could deliver temporary power to certain cooling pumps after cutoff of its steam supply. As a first step, the unit's operators deliberately disconnected the reactor's emergency core cooling system; such a system is necessary because every large reactor core can generate millions or billions of watts of thermal power (heat); this energy must constantly be removed by a flow of coolant, or the core may cause a steam explosion, melt down, or even (in reactors using highly-enriched fuel) a relatively small nuclear explosion. The emergency core cooling system is supposed to keep the core cool when the usual systems have failed. Unit No. 4's operators had not left the emergency core cooling system disconnected, but had committed a series of further errors that allowed the reactor's power output to fall far below planned levels. In attempting to restore the reactor's power output, the operators caused it to go out of control. In a period of approximately 5 seconds, the core's heat output increased exponentially to the point where a steam explosion occurred. This blew a 1,000-ton concrete lid off the reactor and damaged the roof of the reactor hall.

A few seconds later, an even larger explosion occurred when hydrogen released by the breakdown of water exploded. Burning chunks of graphite (a form of carbon of which 1700 tons were present in the reactor core) flew through the air and landed on other parts of the complex, starting fires. The remaining graphite started to burn, releasing a plume of radioactive smoke that was carried by the wind first north, toward Scandinavia, and later west and south over much of the rest of Europe. The graphite fire burned for over a week, but was finally brought under control by firefighters, many of whom died of radiation burns. The reactor was eventually encased in a shell or "sarcophagus" of concrete. In the late 1990s, United States and Ukrainian engineers worked together to evaluate conditions inside the sarcophagus, which may be vulnerable to collapse in an earthquake. The sarcophagus may need to be strengthened to prevent future releases of radioactivity from the site.

The Chernobyl accident is one of the worst nuclear accidents to date, surpassed only by the explosion at the Chelyabinsk-65 plutonium-processing facility in the Ural Mountains in 1957, which was kept secret for decades by

the Soviet Union. Over 20 million curies of radioactive material were lofted into the atmosphere by the Chernobyl explosion and ensuing fire. Some of this material sifted down over nearby towns and countryside, while the rest was spread over Europe by winds, exposing 10 to 20 million people to significant fallout. The number of deaths caused immediately by the accident was in the dozens, but the number of deaths caused in the long term by radiation-induced cancer and other health damage will never be precisely known. Although initially dismissed by experts in the West as exaggerations, reports of 30-to-100-fold increases in thyroid-cancer rates among children in Belarus, northern Ukraine, and parts of the Russian Federation have recently been confirmed.

Nevertheless, the accident could have been worse. Total “meltdown,” in which the molten uranium of the ruined core would have coalesced into a single superheated mass and melted its way down to the groundwater below the plant, causing a violent steam explosion and dispersing even larger quantities of radioactive material, did not occur.

**The role of satellite imagery.** The Chernobyl accident occurred on April 26, 1986, but the Soviet government did not acknowledge the event until April 28 and denied the extent of the disaster for some days thereafter. However, the West quickly had definite knowledge of the accident’s occurrence. Radiation was detected in Sweden the day after the explosion and was soon being monitored by aircraft equipped with radiation-detection devices, including the U.S. Air Force’s 55th Weather Reconnaissance Squadron. Also, Soviet communications were monitored by a geostationary U.S. military satellite called the Vortex, and both military and civilian Earth-imaging satellites were soon in position to image the site. Because of Soviet reluctance to admit observers or release videos, photographs, or accurate announcements about the accident, and because downwind radiation measurements could give no specific information about what was happening at Chernobyl, much news attention in the West focused on the satellite photographs.

The United States’ KH-11 spy satellite provided high-resolution images of Chernobyl to the U.S. government on the afternoon of Tuesday, April 29th, three days after the initial explosion. The KH-11, also known as the Keyhole satellite, was the latest in the KH series of spy satellites that the U.S. began launching in the 1960s, primarily to spy on military activity in the Soviet Union. The KH-11 (whose capabilities were still secret in 1986) could resolve details on the ground down to 4–6 inches (10–15 cm) across. (It has since been replaced by the KH-12 satellite, with a resolution of 2.45 inches [6 cm].) U.S. officials were, therefore, soon as well informed about the Chernobyl accident as vertical views could make them. These images were not, however, released to the public; instead, the

U.S. government’s knowledge was filtered to the media through announcements.

The first civilian satellite to image the accident site was the United States’ LANDSAT, which follows a polar orbit 260 to 570 miles (420 to 912 km) high and takes telescopic pictures of the Earth as it passes beneath. The first LANDSAT (for land-sensing satellite) was launched by the U.S. in 1972, and a series of LANDSATs have been launched as technology has improved. (The seventh LANDSAT in the series is in orbit as of 2003.) LANDSAT images first became available to TV news media on Wednesday, May 3, 1986, only one day after KH-11 images became available to the government. The resolution of the LANDSAT images was comparatively poor, however, being on the order of tens of meters, rather than of centimeters. Nevertheless, they gave visual access to the layout of the reactor complex and cooling pond. Infrared LANDSAT imaging showed both the fire in Unit No. 4 and the chilling of the pond, which indicated that the three remaining reactors in the complex had been shut down.

Several days after the accident, a French satellite named SPOT (for System Probatoire d’Observation de la Terre) was able to provide higher-resolution images to news media. These images were also seen throughout Europe and the United States; on May 1, 1986, for example, ABC news broadcast SPOT infrared photos that showed a plume of hot air trailing from the reactor building.

However, it is doubtful that these nonmilitary satellite images were of any substantive benefit. Despite warnings from professional photo interpreters, announcers on the CBS and NBC television networks announced that the LANDSAT images revealed two reactors on fire, a claim that had to be retracted. Little actual news was derived from the LANDSAT or SPOT images. They served to lessen the sense of mystery surrounding the Chernobyl disaster, but did not supply any specific information that was not already available from other sources. They confirmed—but also, through misinterpretation by amateur analysts, confused—reports already received from official sources.

The KH-11 satellite data, on the other hand, were probably of some utility. They at least gave U.S. officials independent information about the scope of the disaster. However, there was little the West could do with this knowledge. The accident was inside Soviet territory and the response to it was entirely a Soviet affair. Complete cover-up of the event would have been impossible even without spy-satellite imagery, due to the detection of radiation downwind.

Nevertheless, the role of satellite imaging during the Chernobyl accident shows that large-scale disasters can no longer be denied, whether as a whole or in detail, by national governments, given the imaging capabilities of both military and nonmilitary satellites. The basic story of Chernobyl, unlike that of the blowup at Chelyabinsk-65, was public property from the beginning.

## ■ FURTHER READING:

### BOOKS:

Medvedev, Zhores. *The Legacy of Chernobyl*. New York: W. W. Norton & Company, 1990.

Mould, R. F. *Chernobyl Record: The Definitive History of the Chernobyl Catastrophe*. Bristol, England: Institute of Physics Publishing, 2000.

### PERIODICALS:

Alper, Joseph. "Navigating Chernobyl's Deadly Maze." *Science*. 5365 (May 8, 1998): 826–827.

Brugioni, Dino A. "Satellite Images on TV: The Camera Can Lie." *Washington Post*. December 14, 1986.

Williams, Dillwyn. "Cancer after Nuclear Fallout: Lessons from the Chernobyl Accident." *Nature Reviews*, vol. 2 (July, 2002): 543–549.

### SEE ALSO

*Nuclear Power Plants, Security*  
*Russian Nuclear Materials, Security Issues*  
*Satellites, Spy*

## Chile, Intelligence and Security

■ ADRIENNE WILMOTH LERNER

Following a coup on September 11, 1973, Augusto Pinochet assumed power of Chile and for nearly two decades, the dictatorial Pinochet regime created and utilized various intelligence and secret police forces to ferret out and persecute political dissidents. The political prisoners seized by Pinochet's forces became known as the *Desaparecidos*, or Disappeared Ones. Little is known regarding the circumstances of their detainment and subsequent execution, but over 3000 Chilean citizens were killed or disappeared during Pinochet's rule. In 1989, Pinochet lost power in Chile. The subsequent government was left to deal not only with the public memory of the era, but also with a massive restructuring of government agencies, most especially within the intelligence community.

After Pinochet seized power, he established the *Dirección Nacional de Inteligencia* (DINA), or the National Intelligence Directorate in 1974. The agency oversaw military intelligence as well as the national police force. DINA had a paramilitary wing and operated a large secret police force. In 1977, the agency was replaced by the more powerful *Centro Nacional de Información* (CNI), the National Information Center. The CNI performed the same duties as DINA, but also wielded significant judicial powers. No distinction was made between military and civilian accused persons, and the agency directed military tribunals that prosecuted civilians. The CNI was chiefly concerned with internal security, espionage, and protecting

the Pinochet regime. The agency maintained records on private citizens and organizations, often tapping phones and intercepting private wire and written communications. Agents also located and captured persons who fled persecution by escaping to neighboring countries.

After the end of the Pinochet regime, the new government dissolved the CNI in 1990. Many former CNI intelligence agents and members of the secret police were reassigned to military intelligence units or the newly created *Dirección de Inteligencia de la Defensa Nacional* (DIDN), the Directorate of National Defense and Intelligence. Unlike its predecessor agencies, the DIDN is chiefly concerned with defense, not internal intelligence. DIDN coordinates the operations of national intelligence forces, sometimes including military intelligence. Though not without controversy in its own right, the agency seeks to distance itself from the legacy of the CNI and DINA secret police forces.

The role of the Chilean national police forces also changed with government and constitutional reforms in 1980 and 1990. Chile has two main national law enforcement forces, both of which also have roles in the intelligence community. The Carabineros, the national uniformed police, are charged with public safety and border patrols. Under the operational direction of the Ministry of the Interior, the police force is actually part of the Ministry of Defense. The Carabineros also have a paramilitary units and a counterintelligence arm that combat drug trafficking and enforce border security. One branch of the special paramilitary forces, the *Dirección de Inteligencia de Carabineros* (DIC), or Intelligence Directorate, is a counter-subversive intelligence unit charged with fighting terrorism. While laws established protecting the rights of detained persons are largely followed by the police forces, several journalists, citizens, and even legislators have charged some of the Carabineros' paramilitary forces with human rights abuses, including arrest, prolonged detainment, and torture of political dissidents.

The second Chilean police force is the Investigations Police, which employs, among other law enforcement strategies, civilian plain-clothes forces that oversee surveillance and apprehension of suspected criminals and terrorists. The agency investigates serious crime, such as fraud, theft, and murder, and aids the Carabineros with intelligence and investigative work. The Investigations Police maintains airport security and operates the National Identification Bureau, which keeps biographical and criminal records of all citizens and issues national identification cards. Like the Carabineros, the Investigations Police has weathered public suspicion for alleged abuses of power.

Chile has two major advisory boards that address issues of national security, intelligence, and defense. The *Consejo Asesor de Seguridad Interior* (CASI), or Internal Security Advisory Council, is comprised of the Minister of the Interior and various military representatives. CASI advises the executive branch on matters of domestic



security. A second committee the *Consejo Asesor Político-Estratégico* (CAPE), or Strategic Political Advisory Council, monitors defense planning and external security threats.

In the Chilean government, the executive branch has constitutionally granted control over the nation's military, intelligence, and police agencies. However, this power was severely checked by constitutional reforms in 1990. The Carabineros and various military branches are now more autonomous and the president must appeal to his National Security Council, *Cosena*, to remove and replace heads of the various departments and services.

Constitutional and governmental reforms enacted since the early 1980s have radically altered Chilean intelligence and security agencies. As past abuses and atrocities are investigated and brought to light by the international community, especially following the 1999 arrest and detainment of Pinochet on charges of human rights crimes, current Chilean intelligence agencies seek to distinguish themselves from the reputation of their predecessors, despite continuing to hold similarly broad powers with limited legal and administrative restraints.

#### ■ FURTHER READING:

##### BOOKS:

Collier, S., and W. F. Sater. *A History of Chile, 1808–1994*. Cambridge: Cambridge University Press, 1996.

##### ELECTRONIC:

The Government of Chile. <<http://www.gobiernodechile.cl/>> (14 January 2003).

---

## China, Intelligence and Security

---

China is the last communist-dominated world power. The nation reserves veto power on the United Nations Security Council, and is a declared nuclear power. Although censorship and restricted civil liberties persist in China, citizens have witnessed a gradual ease of economic and social restraints. Poverty remains an endemic problem, causing an exodus of people from rural areas into already overcrowded cities. In response, the government prohibited moving between regions and towns without express permission. With the transfer of Hong Kong from British control to Chinese administration in 1997 and the advent of the Internet, the Chinese economy, media, and society have been permeated by Western influences.

In Asia, Chinese politics cast a shadow over smaller satellite states, most especially North Korea. In 2003,

North Korea reactivated a nuclear reactor and announced that it possessed the capabilities to produce nuclear weapons and intercontinental ballistic missiles. The development arose international suspicion that North Korea received nuclear materials and technology from its closest ally, China. The Chinese government denies aiding North Korea, and maintains that it adheres to global non-proliferation efforts. The Chinese intelligence community, however, is reluctant to share information about North Korea with Western nations, especially the United States.

China's main intelligence agency is the Ministry of State Security (MSS). The Communist Party of China dominates the Chinese government, especially the intelligence community. Political espionage within China, and on Chinese citizens, is endemic. Government reforms in 1983 created the MSS, restructuring the Chinese intelligence community and revising the mission of its predecessor agency to account for technological advances in intelligence tradecraft. The MSS utilizes human, signals, remote, electronic, and communications intelligence in its varied operations. The main mission of the MSS is to protect national interests and preserve government stability. However, the MSS also aggressively targets United States and European businesses and factories in a broad campaign of industrial and economic espionage.

Chinese military intelligence is divided into operational departments that fall under the administration of the central government and individual branches of the military. The People's Liberation Army (PLA), China's defense force, maintains trained intelligence, counterintelligence, and security forces. The operations of these forces are highly secret, but most operations deal with domestic and regional threats to the government. PLA intelligence also guards military installations and key assets in the nation's nuclear weapons program. The PLA Navy has its own intelligence force, concentrating on surveillance at sea, signals, and communications intelligence. The PLA Air Force's intelligence forces are known as the Sixth Research Institute. Sixth Research conducts intelligence operations similar to other military and civilian organizations, but is also the primary agency for aerial surveillance.

The Second Intelligence Department focuses on foreign intelligence and espionage against rival nations. In addition to monitoring foreign diplomats and foreign interests within China, the agency also conducts political surveillance of Chinese diplomats abroad. Recently, the Second Intelligence Department received a new mandate to work with the MSS to increase industrial, economic, scientific, and technological espionage efforts, especially in Western nations.

Throughout China there are municipal, regional, and national police forces. The Ministry of Public Security administers the national police force. A military trained police force, Unit 8341 General Security Regiment, provides security for government buildings and personnel, and conducts counterintelligence and anti-terrorism operations. The special police force and intelligence unit is maintained by the General Staff Department.



The Chinese government also maintains secret police forces. These forces are mostly plain-clothes officers who use a network of informers to conduct surveillance and political espionage operations on behalf of the government. Some of these police forces have gained a reputation for their arbitrary imprisonment of citizens and garnered international criticism for use of excessive force and coercion.

A primary duty of China's intelligence and security community is media surveillance and participation in state censorship efforts. The government censors all medium of public expression, but in recent years has placed special emphasis on monitoring electronic communication and the Internet. In 1989, the intelligence forces began monitoring all fax transmissions. Five years later, e-mail communication was declared open to state censorship and surveillance. China's aggressive censorship initiatives monitor political dissidents and anti-government sentiment.

China's news service, Xinhua, provides censored news to China's citizens via television, print media, and radio. The news service also plays a crucial role in China's intelligence community. The bureau analyzes reports from informants, foreign diplomats, foreign journalists and news services, and reports to Chinese government officials. Members of the MSS work within the Xinhua, using its network and journalistic credentials as a mean of gathering intelligence information.

■ FURTHER READING:

BOOKS:

- Ebrey, Patricia Buckley. *The Cambridge Illustrated History of China*. Cambridge University Press, 1999.
- Fewsmith, Joseph. *China since Tiananmen*. Cambridge University Press, 2001.

SEE ALSO

- Clinton Administration (1993–2001), United States National Security Policy*
- Cold War (1945–1950), The Start of the Atomic Age*
- Cold War (1950–1972)*
- Cold War (1972–1989): The Collapse of the Soviet Union Korean War*
- Nixon Administration (1969–1974), United States National Security Policy*
- North Korea, Intelligence and Security*
- North Korean Nuclear Weapons Programs*

---

## Chinese Espionage against the United States

---

■ JUDSON KNIGHT

The question of Chinese espionage against the United States animated policy and intelligence circles during the



In the first case to reach trial under the 1996 Economic Espionage Act, which banned the theft of trade secrets, Hwei Chen "Sally" Yang was found guilty of economic espionage in 1999. AP/WIDE WORLD PHOTOS.

second half of the 1990s, driven by a number of factors, not least of which were allegations that members of the administration of President William J. Clinton had accepted campaign donations from Chinese sources. An investigation by the House Select Committee on U.S. Nuclear Security and Military/Commercial Concerns with the People's Republic of China, chaired by Christopher Cox (R-CA), found that the People's Republic of China (PRC) developed a number of key warheads based on U.S. designs, but failed to establish that this information had come through espionage. Still, the issue of Chinese spying simmered, and finally reached a climactic point with the arrest of Wen Ho Lee, a computer scientist at Los Alamos National Laboratory, in 1999.

In October 1996, the *New York Times*, *Wall Street Journal*, and *Los Angeles Times* ran a number of stories detailing a connection between John Huang, principal deputy assistant secretary of Commerce for International Economic Policy, and Indonesia's Riady family, which had close ties to China. It would eventually be revealed that the PRC had funneled sizeable contributions to the Democratic National Committee through a number of intermediaries. Critics pointed out that, near the same time, the Clinton administration approved the sale of defense satellite technology to the PRC.

Meanwhile, concerns had arisen with regard to Chinese weapons technology, its links with U.S. technology, possible espionage against the United States, and security breaches that had facilitated that espionage. These were the issues that sparked the investigation by Cox's committee in 1998.

The PRC had never been involved in the kind of broadly based espionage on American soil that the Soviet Union had conducted through the KGB and its U.S. agents. The Chinese did, however, have an interest in U.S. technology that had led to efforts at covert acquisition noted as early as 1984, in a report by the Defense Intelligence Agency.

The Cox Report, as the findings of the House committee were called, asserted that the Chinese had appropriated information on seven warheads, including the W88, deployed on the D-5 submarine launched-ballistic missile. This information, the committee concluded, had come from one of the U.S. weapons laboratories operated by the Department of Energy (DOE).

**The investigation.** The House committee completed its seven-month investigation in December 1998, as Clinton's impeachment on unrelated charges loomed (he would eventually be acquitted by the Senate), and published its report in May 1999. In the meantime, the FBI had undertaken an investigation, code-named "Kindred Spirit," of persons who had access to W88 information.

If the Chinese had indeed stolen data on the W88, the theft had occurred in the 1980s, long before Clinton was president; therefore, the results of the Kindred Spirit investigation had nothing to do with Clinton per se. However, the Clinton administration's handling of the situation resulted in continued criticism.

**The Wen Ho Lee incident.** Taiwanese-born computer scientist Wen Ho Lee had been an employee at Los Alamos National Laboratory for 21 years when Energy Secretary Bill Richardson fired him in March 1999. Lee was subsequently arrested by the FBI, charged with not properly securing classified materials and failing to report meetings with individuals from "sensitive" countries, and held for a year. During this time, many observers maintained that Lee was a scapegoat, and some Asian Americans charged that his arrest was motivated by racism. At his trial in September 2000, Lee was convicted on only one of the charges against him—illegally gathering and retaining national security data. Though this was a felony count, the court released him on time served, and ordered him to undergo 60 hours of government debriefing.

Many commentators charged that, if there was an information leak from the Los Alamos lab, and if Lee had anything to do with it, he was only a small part of a much larger problem. Security at the laboratory was considered by many security experts to be inadequate, given the sensitive nature of the work that took place there. For example, in April 2000, two computer drives disappeared

from a high-security area and reappeared two months later behind an office copier in another part of the facility. Security breaches such as these prompted Congress to create the National Nuclear Security Administration (NNSA) as a means of better protecting sensitive properties—and partially removing oversight of those materials from Richardson's DOE.

The title of an article in the *Wall Street Journal* called the Wen Ho Lee case a "diversion," and certainly the case did create more questions than answers concerning Chinese espionage. One of the reasons U.S. authorities have had a difficult time pinning charges of spying on the Chinese is that much of their information seems to have come from open sources. This became apparent with the "discovery" of a 1991 volume, published in Chinese in Beijing, titled *Sources and Techniques of Obtaining National Defense Science and Technology*.

Authors Huo Zhongwen and Wang Zongxiao, both PRC intelligence officers, were frank in stating that Western technical journals "are the first choice of rank and file S&T [science and technology] personnel as well as intelligence researchers." Serendipity, combined with failed security measures, also played a part; in the 1970s, the U.S. government had accidentally declassified more than 19,000 documents on thermonuclear weapons. "This incident," wrote Huo and Wang, illustrates that "...there is a random element involved in the discovery of secret intelligence sources, and to turn this randomness into inevitability, it is necessary that there be those who monitor some sectors and areas with regularity and vigilance." This statement is all the more ironic in light of the fact that a copy of *Sources and Techniques*, which first came to U.S. attention in 1999, had been sitting in the Library of Congress for seven years.

Though the intricacies of the putative Chinese spy scandal in the late 1990s will perhaps never be known, it appears that much of the information the PRC acquired was not a result of subterfuge, but rather of Western openness—and, in some cases, the incompetence of individuals charged with guarding secrets. In any case, the point became all but moot after September 11, 2001. Not only did the United States have far worse concerns than China, but President George W. Bush needed Chinese support for America's war on terror. The issue of Chinese espionage, therefore, was not so much resolved as it was set aside.

#### ■ FURTHER READING:

##### BOOKS:

Cox, Christopher. *U.S. National Security and Military/Commercial Concerns with the People's Republic of China*. Washington, D.C.: U.S. Government Printing Office, 1999.

Stober, Dan, and Ian Hoffman. *A Convenient Spy: Wen Ho Lee and the Politics of Nuclear Espionage*. New York: Simon and Schuster, 2001.

Trulock, Notra. *Code Name Kindred Spirit: Inside the Chinese Nuclear Espionage Scandal*. San Francisco, CA: Encounter Books, 2002.

#### PERIODICALS:

- Broad, William J. "Author to Sue U.S. over Book on China's Nuclear Advances." *New York Times*. (June 18, 2001): A6.
- Gordon, Michael R. "A Dangerous Game." *New York Times*. (April 3, 2001): A1.
- Gosselin, Peter G. "No Sign Drives Left Lab, Richardson Says." *Los Angeles Times*. (June 19, 2000): A3.
- Markoff, John. "Silicon Valley Concern Says It Thwarted Software Theft." *New York Times*. (September 20, 2002): 1.
- Purdy, Matthew, and James Sterngold. "The Prosecution Unravels: The Case of Wen Ho Lee." *New York Times*. (February 5, 2001): A1.
- Richelson, Jeffrey T. "Uncertain Damage." *Bulletin of the Atomic Scientists* 55, no. 5 (September/October 1999): 17–19.
- Rosenthal, Elisabeth. "China Changes Its Approach in the Latest Espionage Incident." *New York Times*. (January 27, 2002): section 1, p. 6.
- Schwartz, Stephen I. "A Very Convenient Scandal." *Bulletin of the Atomic Scientists* 55, no. 3 (May/June 1999): 34–39.
- "The Wen Ho Lee Diversion." *Wall Street Journal*. (September 19, 2000): A26.

#### ELECTRONIC:

China's High-Tech Espionage. Counterintelligence News and Developments/National Counterintelligence Executive. June 2000. <<http://www.ncix.gov/nacic/news/2000/jun00.html>> (March 29, 2003).

#### SEE ALSO

*China, Intelligence and Security Clinton Administration (1993–2001), United States National Security Policy*  
*DOE (United States Department of Energy)*  
*Los Alamos National Laboratory*  
*NNSA (United States National Nuclear Security Administration)*  
*Satellite Technology Exports to the People's Republic of China (PRC)*

## Church Committee

Following the Watergate Scandal, the Senate conducted a thorough review of the function, operation, and administration of the United States intelligence community. A special committee, the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities was established to conduct the sweeping audit of national intelligence services. Known as the "Church Committee" after its chairman Frank Church, the committee investigated not only the actions and operations of the



Former CIA Director William Colby is sworn in to testify before the 1975 Senator Church Committee looking into activities by the intelligence community. ©WALLY MCNAMEE/CORBIS.

intelligence and security services, but also abuses of those services by the Office of the president.

The Church Committee investigated suspected abuses of power by the intelligence community by interviewing hundreds of witnesses and subpoenaing thousands of relevant documents and materials. The main targets of its investigations were the CIA, FBI, National Security Agency (NSA), and Internal Revenue Service (IRS). The committee also closely noted the involvement of the executive branch and President in intelligence affairs.

In 1975 and 1976, the Church Committee issued fourteen reports. Report topics ranged from intelligence and executive branch involvement in the assassination of foreign leaders, an act prohibited by international law, to domestic espionage and political blackmail. Though the committee was initially charged with discovering the abuses of power and intelligence resources that contributed to the Watergate scandal, its investigations encompassed intelligence community operations during the entire post-World War II and Vietnam War era.

The Church Committee issued its final report in April 1976. The Committee concluded that the CIA, FBI, and other intelligence forces, had conducted concerted campaigns of domestic espionage that threatened the Constitutional rights of ordinary citizens. The Church Committee

further decided that such actions could be prevented by the establishment of a permanent means of congressional review for the intelligence community. The Senate created the Senate Select Committee on Intelligence, a modified version of the Church Committee, as an oversight and investigatory committee for the nation's intelligence services. In the 1970s and 1980s, the committee formalized the review and oversight process, and clearly defined instances of abuse of power and illegal activities that warrant committee investigation. The Senate Select Committee on Intelligence continues to operate today.

#### ■ FURTHER READING:

##### BOOKS:

Kurland, Philip B. *Watergate and the Constitution (The William R. Kenan, Jr., Inaugural Lectures)*. Chicago: University of Chicago Press, 1978.

Kutler, Stanley I. *The Wars of Watergate: The Last Crisis of Richard Nixon*. New York: W.W. Norton and Company, 1992.

##### ELECTRONIC:

United States National Archives and Records Administration. Watergate resources. <[http://www.archives.gov/digital\\_classroom/lessons/watergate\\_and\\_constitution/teaching\\_activities.html](http://www.archives.gov/digital_classroom/lessons/watergate_and_constitution/teaching_activities.html)> (01 December 2002).

##### SEE ALSO

*CIA (United States Central Intelligence Agency)*

---

## CIA (United States Central Intelligence Agency)

---

#### ■ JUDSON KNIGHT

The Central Intelligence Agency (CIA) is an independent government organization, founded under the National Security Act of 1947. The agency is a leader among the 14 agencies and organizations in the United States Intelligence Community. The mission of the CIA is to support the president, the National Security Council (NSC), and other officials involved in national security policy by providing accurate, comprehensive, and timely foreign intelligence on national security topics. CIA also supports the chief executive and the national security policy leadership by conducting counterintelligence operations, special activities, and other duties relating to foreign intelligence and national security as directed by the president. The CIA in

the 1990s increased its openness with the American public, and provides relatively detailed information about its organizational structure, through which the director of Central Intelligence (DCI) oversees the four directorates (Administration, Intelligence, Science and Technology, and Operations), as well as numerous other offices.

## Background

CIA's headquarters is in Langley, a neighborhood in McLean, Virginia; hence the term "Langley" is used as a metonym for the entire organization, or its leadership. (The terms "CIA" and "the CIA" are used interchangeably, while "the Company" is a term by which some employees refer to the agency.) Information on its budget is classified, but the entire U.S. intelligence budget, of which CIA comprises but a portion, was \$26.6 billion in 1997, the first year in which such figures were reported. (The 1998 budget figures, the only other ones released as of early 2003, showed an increase of \$100 million, to \$26.7 billion.)

Also classified is the number of persons employed by CIA, but the agency is more open concerning the variety of personnel it hires. There is no one single type of CIA employee, and the popular image of CIA operatives as cutthroats and assassins is a bankrupt cliché. As of 2003, the agency had a particular interest in hiring scientists, engineers, economists, linguists, mathematicians, secretaries, accountants, and computer specialists, although the scope of employment opportunities exceeded even this wide range.

In order to be considered for employment with CIA, an applicant must have a college degree, with a minimum grade point average of 3.0. The applicant must submit to a polygraph and medical examination, as well as background checks. Once hired, the new employee must be willing to relocate to Washington, D.C., or to CIA stations in various locales throughout the world. Many CIA officers work under some form of cover, either as employees of other government organizations (for example, some CIA operatives serve under diplomatic cover in the State Department), or under nonofficial cover, whereby an intelligence officer lives as a private citizen who ostensibly has no ties to the U.S. government.

In accordance with the CIA's mission, the majority of activity by its operatives is directed toward the gathering, production, and analysis of political, economic, and military intelligence on foreign governments, terrorist groups, and criminal organizations. This information originates from documents obtained either openly or illegally, from human sources (human intelligence or HUMINT), from electronic eavesdropping (signals intelligence, or SIGINT), or from images collected by spy cameras or satellites in space (imagery intelligence, or IMINT). Once gathered, intelligence must be processed and analyzed, after which the CIA passes information on to its clients, which include



President Bush, right, and George Tenet, left, head of the Central Intelligence Agency, pause at the entrance to agency headquarters on the way to a speech in March, 2001, in which the president thanked CIA employees for their service and spoke of the importance of intelligence collection and analysis in a world that includes many new threats to U.S. security. AP/WIDE WORLD PHOTOS.

the president and major cabinet-level departments, including State, Defense, and the Treasury.

CIA officers may also be involved in counterintelligence, which is designed to preserve U.S. national security by protecting American assets from foreign spying. Additionally, operatives of the CIA may at times engage in actions such as the spreading of propaganda or disinformation; the use of blackmail or other means to put pressure on enemy operatives; and give support to overseas political or military groups whose objectives align with U.S. interests.

CIA excesses in the past have prompted a number of countermeasures against it on the part of the federal government. In 1975, President Gerald R. Ford issued an executive order forbidding acts of assassination by the CIA, and Executive Order 12333, signed by President Ronald Reagan in 1981, extended this prohibition to forbidding indirect involvement in assassination. This order also expressly prohibited CIA collection of foreign intelligence

on the domestic activities of American citizens. Today, the Executive Office of the president monitors and investigates CIA activities through the president's Foreign Intelligence Advisory Board.

In the mid-1970s, the Church Committee hearings in the Senate and the Pike Committee hearings in the House led to the formation of the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence. Congressional oversight of CIA through these and other committees is an ongoing activity.

Some critics argue that the agency can find ways around the executive and legislative authorities charged with oversight of CIA activities. However, those authorities are privy to information on the CIA far beyond the reach of ordinary citizens lacking an appropriate security clearance and need-to-know, and it is likely that in many cases presidents or legislators have put a stop to activities about which the general public never learned. In light of the increased atmosphere of scrutiny that has attended

CIA activities since the Iran-Contra scandal of the 1980s, the idea that the CIA maintains a government within the government, whereby it exerts its will independent of executive or legislative oversight, is tantamount to conspiracy theory.

## The Structure of CIA

Although both Congress and the president exert oversight of CIA activities, it is the president who holds ultimately authority. Only the president, acting usually through the NSC, can direct the CIA to participate in covert actions. By the same token, DCI reports either directly to the president, or indirectly through the NSC.

Under DCI is the deputy director of Central Intelligence (DDCI), who assists DCI as head of the CIA and of the Intelligence Community. DDCI also exercises the powers of the DCI when the holder of that position is absent or disabled. Within the CIA and the Intelligence Community as a whole, the offices of the DCI and the DDCI are intended to function virtually as a single unit.

**Three lines of authority.** Under the leadership of the DCI/DDCI office are a number of functions within the intelligence community but outside the CIA. These include the DDCI for Community Management and the Assistant DCI for Administration, both of which are statutory positions for which presidential appointment and Senate confirmation is required; the Associate DCI for Military Support; the DCI for Foreign Intelligence Relations; and the National Intelligence Council.

Reporting to the DCI and DDCI are a number of independent offices within the CIA, including the Inspector General, General Counsel (these two are also statutory positions nominated by the president and confirmed by the Senate), Public Affairs, Congressional Affairs, Protocol, and Diversity Plans and Programs. By far the largest chain of command within the CIA, however is the one that runs through the offices of the Executive Director (EXDIR) and Deputy Executive Director (D/EXDIR).

The EXDIR oversees five centers that collectively enable the CIA to carry out its mission: the Chief Financial Officer, Chief Information Officer, Global Support, Human Resources, and Security, each of which have numerous subordinate offices and bureaus. Also under the EXDIR aegis are several independent functions, including the Center for the Study of Intelligence, Office of Equal Employment Opportunity, Ombudsman/Alternative Dispute Resolution, and the Executive Secretary. Finally, the Executive Director's office is in the line of authority between DCI/DDCI and the four directorates.

**The directorates.** The work of the directorates of Operations and Intelligence are at the heart of what most people think

of when they hear the initials "CIA". Operations is responsible for collecting foreign intelligence, including HUMINT, and for overseeing the overt collection of intelligence domestically through persons or organizations that volunteer that information. Within Operations are the Counterintelligence and Counterterrorism centers, the National HUMINT Requirements Tasking Center, and various regional and transnational issues divisions.

The Directorate of Intelligence is responsible for producing the bulk of CIA's finished intelligence, processed from raw data collected in the field. Within this directorate are the offices of Asian, Pacific, and Latin American Analysis; Near Eastern, South Asian, and African Analysis; Russian and European Analysis; Transnational Issues; and Policy Support. Other groups within this directorate include the Collection Requirements and Evaluation Staff, the DCI Crime and Narcotics Center, and the DCI Weapons Intelligence, Nonproliferation, and Arms Control Center.

The Directorate of Administration provides support to CIA activities through a number of administrative and technical offices such as Communications, Facilities and Security Services, Information Technology, and Medical Services. The Directorate of Science and Technology also provides support through research, development, acquisition, and operations of technical capabilities and systems. It directs the Foreign Broadcast Information Service and the National Photographic Interpretation Center.

## A Brief History of the CIA

The CIA began operation on September 18, 1947, with Rear Admiral Roscoe H. Hillenkoetter as its first DCI. In its first covert operation, begun late that year, it influenced the general elections in Italy so as to prevent a Communist victory. Despite this success, President Harry S. Truman blamed Hillenkoetter for failing to predict the coming of the Korean War, and replaced him with General Walter Bedell Smith in October 1950. Under Smith's leadership, the CIA helped bring about the overthrow of Iran's Premier Mohammed Mossadegh after the latter nationalized oil fields in his country.

The accession of Allen W. Dulles to the position of DCI in 1953 marked the beginning of a new era. Under his direction, the CIA became highly energetic and enterprising, building both the Berlin Tunnel and the U-2 spy plane, and undertaking covert operations in Guatemala, Egypt, Indonesia, Chile, and the Congo. Despite a number of successes, the CIA under Dulles also experienced several disasters, most notably the shootdown of U-2 pilot Francis Gary Powers over the Soviet Union in 1960, and the abortive invasion of Cuba at the Bay of Pigs in 1961.

**The 1960s and 1970s.** Under John A. McCone, who replaced Dulles, the CIA regained favor with Kennedy when

it furnished spy plane photos showing Soviet missile emplacements in Cuba, evidence Kennedy used during the Cuban Missile Crisis. Following Kennedy's assassination, President Lyndon B. Johnson appointed fellow Texan William F. Raborn, Jr., who had little background in intelligence. In June 1966, Raborn's DDCI, Richard McGarrah Helms, took the leadership position.

Helms vigorously prosecuted the CIA's secret wars in Vietnam, Cambodia, and Laos, yet struggled with Johnson and President Richard M. Nixon over their demands to conduct domestic intelligence campaigns. Nixon fired him in February, 1973, and after a six-month period in which James R. Schlesinger led the agency, William E. Colby became DCI. Colby's was a difficult tenure, as the CIA came under intense scrutiny from journalists and committees in Congress.

Colby retired in January 1976, and was replaced by future President George H. W. Bush, who put his support behind improvements in satellite technology. When James E. Carter became president, he replaced Bush with Admiral Stansfield Turner, who continued Bush's emphasis on intelligence collection via satellite. Turner sought to distance the agency from its old practices, and covert operations declined dramatically under his leadership.

**From the 1980s to the present.** The inauguration of a new president, Ronald Reagan, in January 1981 brought with it a new DCI, William J. Casey. Under Casey, a veteran of U.S. intelligence in World War II, the CIA's budget, size, and influence grew enormously. Casey directed funds and arms to rebels fighting Communist regimes in both Afghanistan and Nicaragua, and became heavily involved in the Iran-Contra affair. How great that involvement was may never be known, in part because Casey died on January 29, 1987, during the congressional investigation.

William H. Webster, who served as FBI director from 1978 to 1987, succeeded Casey as DCI and served for four years. Under Robert M. Gates, a former DDCI of long standing, the CIA redirected its efforts from a Cold War orientation and toward a focus on issues such as nonproliferation, terrorism, and drug trafficking. During the tenure of R. James Woolsey, appointed in 1993, the CIA came under criticism with the exposure of Aldrich Ames, a mole for the Soviet Union and later Russia, who had operated within of the agency for many years.

Woolsey resigned in January 1995, and John M. Deutch replaced him. Deutch, who held the position for less than two years, was the first DCI to serve on the president's cabinet. In July 1997, George J. Tenet became the fifth DCI in just six years. Though Tenet's leadership style has won praise from observers of the Intelligence Community, the CIA as a whole came under criticism for perceived intelligence failures prior to the September 11, 2001, terrorist attacks. In the wake of those events, the agency has placed a renewed emphasis on human intelligence, or the gathering of intelligence from human sources.

## ■ FURTHER READING:

### BOOKS:

- Andrew, Christopher M. *For the president's Eyes Only: Secret Intelligence and the American Presidency from Washington to Bush*. New York: HarperCollins, 1995.
- Jeffreys-Jones, Rhodri. *The CIA and American Democracy*. New Haven: Yale University Press, 1989.
- Kessler, Ronald. *Inside the CIA: Revealing the Secrets of the World's Most Powerful Spy Agency*. New York: Pocket Books, 1992.
- Prados, John. *President's Secret Wars: CIA and Pentagon Covert Operations Since World War II*. New York: W. Morrow, 1986.
- Richelson, Jeffrey T. *The U.S. Intelligence Community*, fourth edition. Boulder, CO: Westview Press, 1999.
- . *The Wizards of Langley: Inside the CIA's Directorate of Science and Technology*. Boulder, CO: Westview Press, 2001.

### ELECTRONIC:

- Central Intelligence Agency. <<http://www.cia.gov/>> (April 24, 2003).
- Central Intelligence Agency. Federation of American Scientists. <<http://www.fas.org/irp/cia/index.html>> (April 24, 2003).

### SEE ALSO

- CIA, (CSI) Center for the Study of Intelligence*
- CIA Directorate of Science and Technology (DS&T)*
- CIA, Foreign Broadcast Information Service*
- CIA, Formation and History*
- CIA, Legal Restriction*
- DCI (Director of the Central Intelligence Agency)*
- HUMINT (Human Intelligence)*
- IMINT (Imagery Intelligence)*
- Intelligence Community*
- Intelligence, United States Congressional Oversight*
- Iran-Contra Affair*
- NIC (National Intelligence Council)*
- President of the United States (Executive Command and Control of Intelligence Agencies)*
- SIGINT (Signals Intelligence)*
- United States, Intelligence and Security*

---

## CIA (CSI), Center for the Study of Intelligence

---

The Center for the Study of Intelligence (CSI) of the United States Central Intelligence Agency (CIA) is a reference and resource center for scholars and others studying the history and practice of intelligence disciplines. According to CSI's mission statement, the center "seeks to promote study, debate, and understanding of the role of intelligence in American society." This it accomplishes by a number of means, including publications, conferences and seminars, the maintenance of historical records, and

other programs. As of 2003, CSI posted articles from the unclassified, or non-restricted access version, at its Web site.

In accordance with its mission of preserving intelligence history, CSI publishes collections of documents from the Cold War, and conducts oral history projects. It also makes historical records available to scholars and other members of the public. CSI's conference and seminar programs provide a forum for research and discussion, and serve to commemorate major events in the realm of intelligence. An outreach program to institutions of higher learning promotes the teaching of intelligence and related studies. Additionally, CSI sponsors CIA officers-in-residence on selected college and university campuses.

## ■ FURTHER READING:

### ELECTRONIC:

Central Intelligence Agency. "Center for Studies of Intelligence." <<http://www.cia.gov/csi/>> (January 17, 2003).

### SEE ALSO

*CIA (United States Central Intelligence Agency)*  
*United States Intelligence, History*

---

## CIA Directorate of Science and Technology (DS&T)

---

### ■ JUDSON KNIGHT

The Directorate of Science and Technology (DS&T) is one of four directorates within the Central Intelligence Agency (CIA). It provides support to the CIA mission through research, development, acquisition, and operation of technical capabilities and systems. DS&T also directs the Foreign Broadcast Information Service and the National Photographic Interpretation Center (NPIC). Its most notable work, however, is its task as a "spy shop," in which some of the most innovative surveillance technology in history—the U-2 and A-12 spy planes, or the KH-11 and other satellites of the CORONA program—were first envisioned.

### Early History

From the earliest days of CIA, itself created in 1947, scientific and technological support has been an important component of the agency's mission. The earliest ancestor of DS&T was the Office of Reports and Estimates, which in December 1948 merged with the Nuclear Energy Group of the Office of Special Operations to form the Office of Scientific Intelligence (OSI). The latter would remain the CIA's principal scientific research laboratory until 1962.

In researching his book on DS&T, *The Wizards of Langley* (2001), intelligence scholar Jeffrey T. Richelson accessed a host of documents that were once highly sensitive, but are now declassified. He posted a number of these at a permanent Web site associated with the George Washington University National Security Archive. One notable early example from the collection is a November 5, 1954, letter from Polaroid chief executive officer Edwin Land to Director of Central Intelligence (DCI) Allen Dulles, urging him to develop a specialized aircraft that could fly at high altitudes and obtain ultra-high resolution photographs. From this letter and other early discussions would come the U-2, developed at Lockheed's Skunk Works facility in California.

Other documents from the 1950s show early CIA plans for the deployment of the first spy satellites. At that time, the Air Force had its own satellite project in the works, but the CIA's CORONA, launched in 1959, would prove much more successful, and would outlast the Air Force SAMOS program by a decade. Much less successful were CIA experiments with psychotropic drugs, including LSD, during the period 1949–1963. Richelson excerpted a January 1975 memo, written just before the CIA became the target for a series of congressional investigations, detailing those experiments, including the infamous MKULTRA program.

**The 1960s.** In 1962, OSI became the Deputy Directorate for Research, whose name was again changed to Deputy Directorate for Science and Technology in 1963. The directorate assumed its present name in 1965. During this period, the agency developed the A-12 Oxcart, which, though successful, never equaled the U-2 for accuracy. Its satellite programs continued to progress, yet as an NPIC photographic interpretation report from August 1962 showed, even the KH-4 satellite did not offer imagery any better than that obtained by the U-2.

A March 1967 memo, from which several details (including the recipient) were excised, provides an illustration of the folly that sometimes befell DS&T. The memorandum describes a project known as "Acoustic Kitty," whereby DS&T attempted to develop a mobile eavesdropping platform using a cat that had been surgically altered by cutting it open, inserting batteries, and wiring its tail to become an antenna. The unfortunate creature was run over by a taxi before it could be trained for its mission.

**The 1970s.** More indicative of DS&T's involvement in cutting-edge technology was a report from a June 1971 meeting of the president's Foreign Intelligence Advisory Board in which President Richard M. Nixon, along Land (still highly involved with the Intelligence Community) and others, discussed the idea of developing a satellite that could return images in real time. Today, of course, such a concept is well known, but in an era when satellites still recorded images on film for viewing days or weeks later, the idea of a satellite that could instantaneously



relay images to a ground station seemed farfetched. In December 1976, the vision discussed at this meeting was realized with the deployment of the KH-11 satellite.

Once again, documents selected by Richelson illustrate juxtaposition of scientific triumph with less successful undertakings. Even as KH-11 was being born, DS&T undertook experiments in "remote viewing," or the use of purported psychic knowledge to explore targets of interest that could not be glimpsed by ordinary means. According to a December 1975 report from Los Alamos Scientific Laboratory, remote viewers "saw" a number of objects that, as shown by satellite photography, were not at the site in question. After the end of the Cold War, American scientists visiting the site discovered that it was being used to develop a nuclear-powered space rocket and not—as remote viewers had supposed—for underground nuclear tests.

## DS&T Today

Information about more recent DS&T activities is necessarily scanty, but these details from the first 30 years of CIA science and technology illustrate the breadth of activities with which it was associated in the past. As of 2003, the DS&T is tasked with collecting, assessing, and exploiting information to assist the agency in the execution of its mission by applying innovative scientific, technical, and engineering solutions to critical intelligence matters.

The workforce of DS&T incorporates some 50 different disciplines, ranging from computer scientists to engineers to linguists. These specialists develop, design, evaluate, and deploy highly specialized equipment intended to provide the United States with a significant advantage in intelligence and special operations.

DS&T is involved in a whole range of functions that support the entire intelligence cycle. These activities include collecting information and materials of intelligence value from foreign open sources, developing and deploying collection systems against the most challenging intelligence targets, supporting the National Reconnaissance Office in creating efficient satellite systems, providing state-of-the-art technologies for the clandestine collection of intelligence, and researching and developing advanced technologies to provide and maintain an advantage for the United States. In pursuit of these activities, DS&T in 2001 developed In-Q-Tel, a nonprofit corporation intended to seek information technology solutions to critical needs faced by CIA as a whole.

### ■ FURTHER READING:

#### BOOKS:

Jeffreys-Jones, Rhodri, and Christopher M. Andrew. *Eternal Vigilance? 50 Years of the CIA*. Portland, OR: Frank Cass, 1997.

Richelson, Jeffrey T. *The U.S. Intelligence Community*, fourth edition. Boulder, CO: Westview Press, 1999.

———. *The Wizards of Langley: Inside the CIA's Directorate of Science and Technology*. Boulder, CO: Westview Press, 2001.

#### PERIODICALS:

Goodman, Melvin A. "Science at the CIA." *Issues in Science and Technology* 18, no. 3 (spring 2002): 90–93.

Mooney, Chris. "Spy Tech." *The American Prospect* 13, no. 2 (January 28, 2002): 39–41.

Prados, John. "Understanding Central Intelligence." *Bulletin of the Atomic Scientists* 58, no. 2 (March/April 2002): 64–65.

#### ELECTRONIC:

Directorate of Science and Technology. Central Intelligence Agency. <<http://www.cia.gov/cia/dst/home.html>> (April 24, 2003).

Richelson, Jeffrey T. Science, Technology and the CIA. National Security Archive, George Washington University. <<http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB54/index2.html>> (April 24, 2003).

#### SEE ALSO

*Antiballistic Missile Treaty*  
*Aviation Intelligence, History*  
*Biochemical Assassination Weapons*  
*CIA (United States Central Intelligence Agency)*  
*CIA, Foreign Broadcast Information Service*  
*Dual Use Technology*  
*Movies, Espionage and Intelligence Portrayals*  
*Photographic Interpretation Center (NPIC), United States National*  
*Pseudo Science Intelligence Studies*  
*Psychotropic Drugs*  
*Satellites, Spy*  
*U-2 Spy Plane*

## CIA, Foreign Broadcast Information Service

### ■ MARTIN J. MANNING

The Foreign Broadcast Information Service (FBIS) is the pre-eminent collector of open source information for the United States government; it collects, translates, and disseminates foreign open source material for U.S. Government use. It started as the Foreign Broadcast Monitoring Service (FBMS), established in the Federal Communications Commission (FCC) by a presidential [Franklin D. Roosevelt] directive on February 26, 1941, to monitor, record, transcribe, and analyze foreign broadcasts. The FBMS was organized after assistant secretary of state Breckinridge Long became concerned about the possible loss of diplomatic reporting and other information if the war in Europe caused American embassies to close. Long suggested radio as a supplemental source of intelligence

and looked to the FCC, which regulated domestic radio, as the best source to further monitor foreign broadcasts.

The FBMS was changed to the Foreign Broadcast Intelligence Service by FCC order on July 28, 1942. Its principal activities included translations of monitored foreign broadcasts; transmission of telegrams and cablegrams to government agencies concerned with war propaganda; and the preparation of daily reports by the Far Eastern, Latin American, and European Sections, with weekly reviews of official foreign broadcasts and radio reports on the Far East. The FBMS's first director, 1941–1943, Harold N. Graves, Jr., directed the FBMS's predecessor, Princeton Listening Center, which was launched in November 1939 at Princeton University with funding from the Rockefeller Foundation. It was the U.S. pioneer in the systematic monitoring, translation, and analysis of broadcasts from Berlin, London, Paris, Rome, and Moscow. One journalist described the FBMS as the "greatest collection of individualists, international rolling stones, and slightly batty geniuses ever gathered together in one organization."

The FBIS's first analytic report, released on December 6, 1941, warned of Tokyo's increasingly belligerent tone. The next day, the Japanese attacked the U.S. Navy fleet at Pearl Harbor in Hawaii, initiating the U.S. entry into World War II. The FBIS became responsible for providing open-source intelligence (OSINT) as its part of the military and civilian wartime intelligence effort. On January 14, 1943, FBIS issued its first special report on Nazi propaganda, prepared by the Analysis Directorate's German Section. FBIS maintained a special telephone connection to the White House, and on September 10, 1943, when Hitler went on the air in reaction to Italy's surrender, eager listeners on the line included British Prime Minister Winston Churchill, U.S. Army Chief of Staff General George C. Marshall, and Roosevelt's advisor Harry Hopkins.

After World War II, the FBIS was transferred to the Military Intelligence Division, War Department General Staff, by order of the secretary of war in January 1946, pursuant to an agreement between the FCC and the War Department. The first issue of the *Daily Report* was published the same month. After a period, as part of the Central Intelligence Group (CIG), National Intelligence Authority, the FBIS became part of the newly created Central Intelligence Agency (1947) and negotiated with the British Broadcasting Corporation (BBC) to divide monitoring responsibilities of most of the world's pertinent news broadcasts of interest to intelligence analysts.

As of 2003, the FBIS continues to monitor, translate, and republish selected foreign radio and television broadcasts, newspaper articles, government news agency releases, and political speeches. The selection of items to be included has been determined by the needs of its primary users, officials of the U.S. government. Political, military, economic, and environmental topics are the major emphases. The translations have been published as quickly as possible, usually within a few days of original publication, in a series of daily reports. Since 1996, the service has

been available online through a Worldwide Web site known as the World News Connection and through its website: <<http://www.fbis.gov>>.

Foreign newscasts, as well as documentaries and investigative news programs, are the mainstay of the FBIS global television collection. The material FBIS disseminates is known as "FBIS Reporting" and is assumed to be copyrighted by the foreign originator. Contractual and copyright obligations requires that the information be restricted to official U.S. government use.

From its first, unprepossessing headquarters at 316 F Street, NE, in downtown Washington, the FBIS now resides in more lavish buildings in Reston, Virginia, where it operates 24 hours a day, seven days a week, in the CIA's Directorate of Science and Technology.

#### ■ FURTHER READING:

##### BOOKS:

Graves, Harold N. *On the Short Wave*. New York: Foreign Policy Association, 1941.

##### PERIODICALS:

Mercado, Stephen C. "FBIS against the Axis, 1941–1945: Open-Source Intelligence from the Airwaves." *Studies in Intelligence* no. 11 (Fall-Winter 2001): 33–43.

##### ELECTRONIC:

National Technical Information Service, Department of Commerce. "World News Connection" 2002. <<http://wnc.fedworld.gov/>> (March 20, 2003).

##### SEE ALSO

*COMINT (Communications Intelligence)*  
*Communications System, United States National*

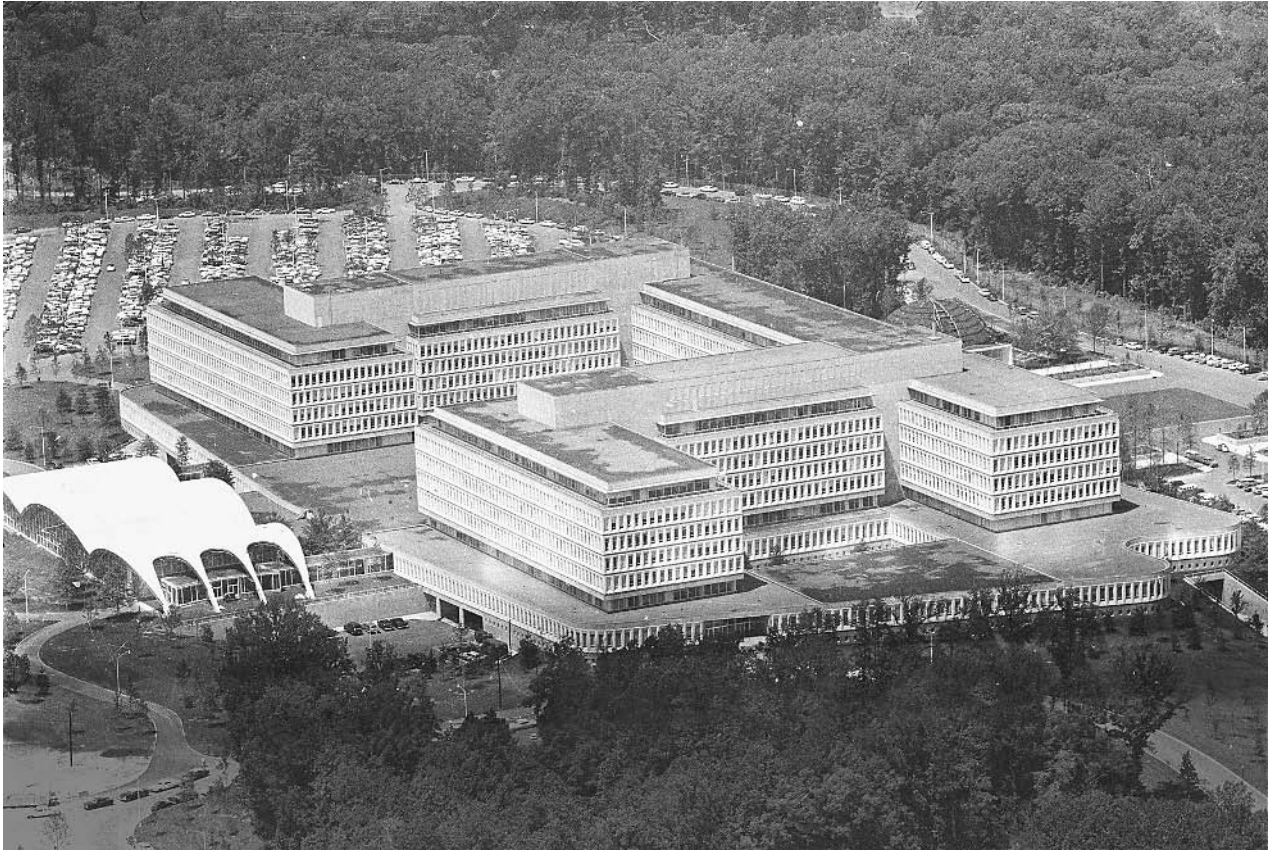
---

## CIA, Formation and History

---

#### ■ MICHAEL J. O'NEAL

United States military planners had always relied on intelligence during wartime, but it was not until World War II that the U.S. government began collecting intelligence systematically. Even before the Japanese attack on Pearl Harbor on December 7, 1941, President Franklin D. Roosevelt had been having doubts about the effectiveness of the nation's intelligence-gathering efforts because they were scattered among the various branches of the military. To correct this deficiency, he appointed William J. Donovan, a New York lawyer who had won the Congressional Medal of Honor as an Army colonel in World War I, to put together a plan for an intelligence service. Out of Donovan's plan emerged the Office of Strategic Services (OSS)



An aerial view of the Central Intelligence Agency (CIA) headquarters in Langley, Virginia, about eight miles from downtown Washington, D.C. AP/WIDE WORLD PHOTOS.

in June 1942. The OSS, under Donovan's leadership, was given the task of collecting and analyzing information needed by the Joint Chiefs of Staff, the heads of all the branches of the nation's military, and to conduct special or clandestine operations that were not carried out by other federal agencies or branches of the military. Throughout the war, the OSS provided policy makers and the military with essential intelligence, including enemy troop strength estimates, that was crucial to planning military campaigns.

In the months and years following World War II, policy makers struggled with two questions: Who should conduct the nation's intelligence-gathering activities? And who should supervise their efforts? These were important questions, for the Cold War rivalry between the United States and its chief adversary, the Union of Soviet Socialist Republics, or Soviet Union, made accurate and timely intelligence about Soviet intentions imperative. Initially, President Harry S. Truman favored dividing responsibilities between military and civilian agencies. In October 1945, he abolished the OSS and transferred its operations to the Departments of War and State. At about the same time, Donovan proposed the formation of a strictly civilian organization that would coordinate intelligence gathering. Such an organization would be authorized to conduct subversive operations abroad, but it would have no police

or law-enforcement authority at home. Donovan's plan met with resistance from both the military and the Federal Bureau of Investigation, which feared that the plan would lessen their influence. In January, 1946, Truman struck a middle course. He established the Central Intelligence Group (CIG), giving it the authority to coordinate intelligence gathered by existing departments and agencies. The CIG was placed under the supervision of a National Intelligence Authority, which in turn was made up of the president and the secretaries of the State, War, and Navy departments. For the first time in its history, the United States had a peacetime intelligence organization.

The original CIG and the National Intelligence Authority lasted less than two years. In 1947, Congress entered the picture by passing the National Security Act. This act created the National Security Council (NSC) and placed under its authority the Central Intelligence Agency (CIA). Intelligence gathering was now firmly under the control of civilian authorities, principally the president and his NSC staff.

**The growth of the CIA.** Throughout the early years, the structure of the CIA changed and its functions were assigned and reassigned to various departments. By the

early 1960s, its broad structure had become largely what it is in 2003. Under the supervision of the Director of Central Intelligence (DCI), one of any president's chief political appointees, are four major departments, or directorates. The Directorate of Administration supervises the business aspects of the agency, including personnel, logistics, training, and the like. The Directorate of Intelligence is the CIA's analysis arm; it interprets raw information and turns it into useful intelligence for the president and the NSC. The Directorate of Science and Technology employs top scientists to develop ever more sophisticated scientific tools to aid in the intelligence-gathering process. Finally, the Directorate of Operations is the traditionally glamorized component of the CIA, for its agents conduct actual intelligence operations in the field.

In its early years, the staff of the CIA consisted primarily of former OSS personnel. Until recent years, the CIA was overwhelmingly a male domain, including mostly academics, lawyers, and journalists. At the time, the CIA had a distinctly academic tone, for the agency recruited top students from the nation's most prestigious universities and placed considerable emphasis on the sober analysis of information. In 1950, the CIA employed about 5,000 people who were housed in various locations in and around Washington, D.C. In 1961, the CIA moved into its current headquarters in Langley, Virginia, and continued to grow. Today the exact number of CIA employees is classified (about 20,000; 6,000 of whom serve in clandestine areas of the organization), but one measure of the agency's size is the nation's budget for intelligence-gathering activities, which in 1998 was \$26.7 billion.

In the 1950s and early 1960s, the CIA enjoyed considerable prestige, for it was primarily through intelligence that the United States resisted the expansion of the Soviet Union and the spread of Communism. The CIA, for example, revealed the presence of Soviet nuclear missiles in Cuba during the 1962 Cuban missile crisis. In the 1960s, however, the CIA began to endure some public opinion scrutiny. In 1961, it backed the disastrous Bay of Pigs operation intended to overthrow Cuban dictator Fidel Castro. Later in the decade, as opposition to the war in Vietnam grew, the CIA was seen in many quarters as emblematic of a misguided foreign policy. Further damaging the agency's reputation were revelations that it took part in unsavory operations in Central and South America, often undermining unfriendly regimes and propping up brutal dictators who were friendly to American interests. In 1975, Senator Frank Church led congressional hearings that resulted in restrictions to the entire intelligence community concerning domestic spying and the implementation of stricter oversight of covert operations abroad. Because of these hearings and revelations, the CIA spent much of the 1980s and 1990s refurbishing its image. After the terrorist attacks of September 11, 2001, the CIA took on added luster as the nation looked to the agency as the front line in the fight against terrorism. In the wake of the terrorist attacks, the CIA was again granted increased

funding and operational authority to pursue counter-terrorism actions.

**Directorate of Science and Technology.** In its early years, the CIA relied primarily on field operations, but in the early 1960s Director John A. McCone, whose tenure as DCI ran from 1961 to 1965, concluded that the CIA of the future would have to rely more on science and technology. Until that time, the CIA's science and technology efforts had been scattered among various directorates. With the emergence of "overhead" intelligence-gathering technology, including the U-2 spy plane and reconnaissance satellites, McCone gathered all of the agency's scientific and technological capabilities under one roof. The result was the formation of the Directorate of Science and Technology (DS&T) in 1963. Among the DS&T successes are the design and development of high-tech imagery and eavesdropping satellites, including the KH-11 and RHYOLITE. It monitored Soviet missile capabilities from ground stations in China, Norway, and Iran. Its photographic experts played a key role in monitoring such events as the Chernobyl nuclear power plant disaster in the Soviet Union in 1986 and Iraqi troop movements during the 1991 Gulf War. Many of the DS&T's innovations, including heart pacemaker technology, have had implications for medical research.

#### ■ FURTHER READING:

##### BOOKS:

- Ranelagh, John. *The Agency: The Rise and Decline of the CIA*. New York: Simon and Schuster, 1986.
- Richelson, Jeffrey T. *The Wizards of Langley*. Boulder, Colo.: Westview, 2001.
- Troy, Thomas F. *Donovan and the CIA: A History of the Establishment of the Central Intelligence Agency*. Frederick, MD.: University Publications of America, 1981.

##### ELECTRONIC:

- Central Intelligence Agency. "Key Events in CIA's History." <<http://www.cia.gov/cia/publications/facttell/keyevent.htm>> (January 2, 2003).
- Federation of American Scientists. "Central Intelligence Agency." September 23, 1996. <<http://www.fas.org/irp/cia/ciahist.htm>> (January 2, 2003).

##### SEE ALSO

- Bush Administration (1989–1993), United States National Security Policy*
- Bush Administration (2001–), United States National Security Policy*
- Church Committee*
- CIA (United States Central Intelligence Agency)*
- CIA (CSI), Center for the Study of Intelligence*
- CIA Directorate of Science and Technology (DS&T)*
- CIA, Foreign Broadcast Information Service*
- CIA, Legal Restriction*
- Covert Operations*
- United States, Counter-Terrorism Policy*



James Angleton, former chief of Counterintelligence at the Central Intelligence Agency, answers questions before the Senate Intelligence Committee in 1975 regarding the CIA practice of opening mail of targeted Americans. Proceedings from the committee resulted in tighter controls concerning CIA covert actions. AP/WIDE WORLD PHOTOS.

## CIA, Legal Restriction

■ JUDSON KNIGHT

Although created by legislation in 1947, the Central Intelligence Agency (CIA) operated largely free of legal restrictions for about a quarter-century. This all changed in the early 1970s, when CIA involvement in the Watergate break-in led to investigations in Congress. Simultaneous with this was a series of revelations in the media concerning CIA covert operations in the past, which only further influenced a widespread opinion that the agency had operated for too long without benefit of legal oversight. The result was the formation of House and Senate intelligence committees, as well as other restrictions that have served—with varying degrees of success—to put the agency under legal restraint.

**Excesses and reactions.** The National Security Act, passed by Congress in 1947, formally established the CIA, even though a presidential directive signed by President Harry S. Truman in January 1946 had established a forerunner,

the Central Intelligence Group. The Central Intelligence Agency Act of 1949, rather than limiting the powers of the agency, gave it a virtual blank check: CIA budgets, salaries, and even job titles would be secret; contracts could be awarded without bidding; and the CIA could grant permanent residency to aliens—particularly defectors from the Soviet bloc—and their families.

During the height of the Cold War, the CIA operated with a greater degree of operational freedom. Only in the 1970s, as the Cold War entered a new phase of detente, and as the American public became increasingly suspicious of their government, did the agency come under increased scrutiny and hence, legal restriction. More than even the Vietnam War, the single greatest factor in spawning this distrust was the 1972 Watergate break-in, in which CIA personnel were involved. Watergate, which would lead to the downfall of the Nixon administration, started the CIA on a spiral of diminishing public confidence that would lead to the imposition of greater legal restrictions on the agency.

Just as *Washington Post* journalists Bob Woodward and Carl Bernstein broke the Watergate story, Seymour Hersh of the *New York Times* started a barrage of investigative reports directed at the CIA when in December, 1974

he uncovered evidence of a lengthy domestic intelligence campaign involving interception of private mail. In the years that followed, the public would learn that the agency had been involved in assassinations and attempted assassinations, conducted experiments using LSD and other psychotropic drugs, and lied to the public concerning the development of secret spy planes.

**New committees and executive orders.** In response to the growing public distrust of the CIA, President Gerald R. Ford on January 4, 1975, signed Executive Order 11828, which created the Commission on CIA Activities, to be chaired by Vice President Nelson Rockefeller. On January 27, the Senate established its Select Committee to Study Governmental Operations with Respect to Intelligence Activities, under the leadership of Frank Church (D-ID). The House of Representatives created its own Select Committee on Intelligence, later chaired by Otis G. Pike (D-NY), on February 19.

The Church Committee submitted its final report on April 26, 1976. Meanwhile, on January 29, just two days before the Pike Committee was to complete its investigation, the House voted not to make its findings public. (The report was eventually leaked to journalist Daniel Schorr, and published in the *Village Voice*.) The Church Committee had already begun to have an impact, and as of May 19, the Senate had put in place its permanent Select Committee on Intelligence. On July 14, 1977, the House established its own such committee.

Ford signed Executive Order 11905, "United States Foreign Intelligence Activities," on February 18, 1976. The order established the Committee on Foreign Intelligence and the Operations Advisory Group, which greatly increased executive oversight of the CIA. The National Security Council (NSC), established at the same time as the CIA, also afforded this oversight, but in the NSC, the Director of Central Intelligence primarily acted in the capacity of an intelligence advisor, whereas the new committees extended the President's involvement in CIA budget planning and resource allocation.

President James E. Carter, on January 24, 1978, signed Executive Order 12036, which changed the shape of the intelligence structure. Among its provisions was a restriction of bugging and domestic surveillance activities, and guidelines whereby the CIA could request surveillance authorization through the Federal Bureau of Investigation. This order was superseded on December 4, 1981, by Executive Order 12333, in which President Ronald Reagan further clarified legal oversight of the intelligence community.

**Laws in the early 1980s.** The effort to bring the CIA into line continued with a series of congressional acts in the early 1980s, including the 1980 Intelligence Oversight Act. The act replaced the armed services committees as the principal arm of legislative oversight for the CIA in both houses

of Congress. Thenceforth, the newly formed intelligence committees would take the lead, though the armed services committees remain involved in monitoring intelligence activities, as did the foreign relations and foreign affairs committees. At its end, the CIA maintains an Office of Congressional Affairs, and provides more than a thousand briefings to Congress, its committees, and their staffs, each year.

In an effort to prevent the pendulum from swinging too far in the opposite direction, Congress passed the Intelligence Identities Protection Act. The act, which Reagan signed into law on June 23, 1982, made it a felony to reveal the names of covert intelligence personnel. On October 15, 1984, Reagan signed the Central Intelligence Agency Information Act, which exempted the agency from the search and review requirements of the Freedom of Information Act. (The latter, passed in 1967 and amended in 1975, had further increased U.S. citizens' protection against domestic intelligence operations by the CIA and other groups.)

**Striking a balance.** All issues of legal authority over the CIA were not solved in the period from the mid-1970s to the early 1980s, however. Still ahead lay the Iran-Contra debacle, which did not so much lead to new legislation as it further eroded the trust of lawmakers and the public toward the CIA. As a result, by the early 1990s, the U.S. intelligence community found itself so restricted that it could hardly conduct its operations. This fact hit home after the terrorist attacks of September 11, 2001, when it became apparent that a lack of human intelligence had contributed to the government's failure to foresee the attacks. However, the post-September, 2001 emphasis on security portended a relaxation of restrictions on CIA activity.

#### ■ FURTHER READING:

##### BOOKS:

- Legislative Oversight of Intelligence Activities: The U.S. Experience: Report.* Washington, D.C.: U.S. Government Printing Office, 1994.
- Polmar, Norman, and Thomas B. Allen. *Spy Book: The Encyclopedia of Espionage.* New York: Random House, 1998.
- Richelson, Jeffrey T. *The U.S. Intelligence Community*, fourth edition. Boulder, CO: Westview Press, 1999.

##### PERIODICALS:

- Cannon, Carl M. "Central Intelligence Agency." *National Journal* 33, no. 25 (June 23, 2001): 1903–1904.

##### SEE ALSO

- CIA (United States Central Intelligence Agency)*  
*CIA, Formation and History*  
*FOIA (Freedom of Information Act)*  
*HUMINT (Human Intelligence)*  
*Intelligence, United States Congressional Oversight of Intelligence Authorization Acts, United States Congress*

NSC (National Security Council)  
 PFIAB (President's Foreign Intelligence Advisory Board)  
 President of the United States (Executive Command and  
 Control of Intelligence Agencies)

Singh, Simon. *The Code Book*. New York: Doubleday, 1999.

SEE ALSO

*Cipher Machines*  
*Codes and Ciphers*  
*Enigma*

## Cipher Disk

A cipher disk is a handheld coding device for generating a limited number of substitution ciphers, that is, ciphers in which each letter of the regular alphabet is enciphered as a single character from a cipher alphabet. A typical cipher disk consists of an inner ring with the characters of the regular alphabet printed around its outer edge, and an outer ring that fits snugly around the inner ring and can be rotated. Around the outer ring is printed a cipher alphabet that has the same number of characters as the regular alphabet. This cipher alphabet may consist of a scrambled regular alphabet or of other symbols. To encipher a message, the user of the cipher disk first chooses some particular alignment of the outer ring with the inner ring. For example, if the cipher alphabet consists of the numbers 1 through 26 (in order), the user may align the number 10 on the outer ring with the letter A on the inner ring. The letter A will then encipher as 10, the letter C as 12, the letter Z as 9, and so forth. By shifting the outer ring one or more letter-positions, the user obtains a different substitution cipher. Some cipher disks have an internal mechanism that advances the outer ring by one step after the encipherment of each letter; this prevents a given plaintext letter from always enciphering as the same ciphertext letter.

The earliest known description of the cipher disk was penned by Italian artist Leon Battista Alberti (1404–1472) in 1470. Cipher disks produce ciphers that are too simple for practical use in the modern world, but were used in the field by Confederate forces during the United States Civil War (1861–1865). Union cryptographers, however, often had no problem reading the Confederacy's encrypted messages. Cipher disks were also widely distributed in the U.S. in the 1940s as marketing giveaways for radio adventure programs such as *Captain Midnight*. These programs were popular even with adults, including active air crews during World War II, and stories—possibly apocryphal—have circulated claiming that combat forces occasionally put the toy cipher disks to real-life use. More complex ciphering systems based fundamentally on the cipher disk concept, such as Enigma, have seen extensive real-world service.

■ FURTHER READING:

BOOKS:

Deavours, Cipher, et al. *Cryptology: Machines, History & Methods*. Norwood, MA: Artech House, 1989.

## Cipher Key

A cipher key is a sequence of symbols that a user of a given cipher system must possess in order to use the system. Without a key, a user cannot encipher messages (turn them from plaintext to ciphertext) or decipher messages (turn them from ciphertext to plaintext).

Keys greatly enhance cipher security and are a feature of all modern ciphers. To see the value of keys, consider the following Caesar shift cipher:

Plaintext alphabet:  
 ABCDEFGHIJKLMNOPQRSTUVWXYZ  
 Ciphertext alphabet:  
 DEFGHIJKLMNOPQRSTUVWXYZABC

Note that the ciphertext alphabet is merely the plaintext alphabet shifted to the left by three letter-positions (with A, B, and C wrapped around to the right). As it stands, this cipher has no key; it consists of a one-step method that never varies (e.g., in reading the above table, E from the Plaintext alphabet always enciphers to H of the Ciphertext alphabet, the E being directly below the H in the table). Ciphers such as this example are easy to break. Twenty-four similar, but distinct ciphers can be generated, however, simply by shifting the lower alphabet by some number of positions other than three. For example, a left-shift of six letters changes the ciphertext alphabet to GHIJKLMNOPQRSTUVWXYZABCDEF. One can therefore imagine a cipher system in which one specifies a different shift before enciphering each message. The receiver will also need to know the shift, so that they can use the same substitution cipher that the sender used. In this improved cipher, the shift number for each message would function as a *key*. There are 25 possible keys (i.e., shifts) in this system, each of which would cause a different ciphertext to be produced from a given plaintext. This is a general feature of keys: a key modifies the rules for producing or deciphering ciphertext.

In general, an opponent who obtains a key (and who understands the rest of the cipher system) can decipher all the plaintext that has been enciphered using that key. In the example above, there are only 25 possible keys, and the cipher can easily be attacked by exhaustion, that is, by trying all possible keys. In real-world cipher systems, the

number of keys is made too large for exhaustion to be practical. For example, if a 56-bit binary number is used as the key, there are  $2^{56} > 7.2 \times 10^{16}$  possible keys. An ideal cipher would be breakable only by exhaustion; in practice, ciphers almost always have subtle weaknesses that make it possible to break them without having to guess all possible keys.

## ■ FURTHER READING:

### BOOKS:

Mollin, Richard A. *An Introduction to Cryptography*. New York: Chapman & Hall, 2001.

### SEE ALSO

*Codes and Ciphers*

---

## Cipher Machines

---

### ■ LARRY GILMAN

A cipher machine is a mechanical device that assists in the production of ciphertext from plaintext and vice versa. In this broad sense, any mechanical aid from a cipher wheel to a supercomputer can qualify as a cipher machine; however, the term is usually reserved for devices that are fairly complex and that operate on mechanical or electromechanical rather than on electronic principles.

Before World War I, ciphers were implemented using either marks on paper or simple aids such as cipher wheels. After the war, a number of inventors in various countries produced cipher machines that transferred the complexity and tedium of ciphering to a mechanism. These machines allowed the operator, who might be completely ignorant of the cipher's nature, to simply type at a keyboard or enter characters one by one by moving a wheel with their fingers. If plaintext (ordinary written language) was entered into such a machine, ciphertext (apparently random characters) was produced; if ciphertext was entered, plaintext was produced. Cipher machines made it possible to cipher and decipher large numbers of messages with less training for personnel, fewer errors, and higher speed.

Many cipher machines invented in the post-World War I period employed as their key component the scrambler disk or rotor. The typical rotor is a disk a few inches in diameter, with letters and numbers printed around its rim and embedded wires connecting one side to the other. Matching points on opposite surfaces of the disk correspond to the same alphanumeric characters, and each wire running through the disk corresponds to one character to be enciphered or deciphered. By connecting one point on surface A of the rotor—say, the point corresponding to the letter M—to a different point on surface B—say,

the point corresponding to the letter Z—the rotor implements a fixed substitution cipher (i.e., replaces every character by some other). In this example, M is enciphered to Z and Z is deciphered to M (or vice versa).

The substitution cipher built into the wires of a single rotor is a trivial one. What the inventors of the rotor-based cipher machines realized was that by lining up multiple cipher disks and continually rotating them as a message was enciphered or deciphered, they could produce much more formidable ciphers. For instance, three rotors could be stacked or aligned so that surface B of rotor 1 met surface A of rotor 2, while surface B of rotor 2 met surface A of rotor 3. Each letter of the input (at surface A of rotor 1) then follows a tortuous path through the wiring of all three disks to the output (at surface B of rotor 3). If the rotors are shifted upon encryption or decryption of each and every message character, the encryption/decryption path is not only tortuous, but also changing. A degree of cipher security that was essentially impossible with pencil-and-paper ciphering was made possible by such machines.

The rotor principle was discovered independently by inventors in several countries, the most famous being German engineer Arthur Scherbius (1878–1929). Scherbius invented a three-rotor cipher machine, the Enigma, in 1918 (the last year of World War I). Scherbius tried unsuccessfully to sell his machine to commercial buyers, but he was ahead of his time; corporations did not begin to use encryption widely until the 1960s. Enigma was, however, purchased by the German government in 1926. At that time, Germany was busy rebuilding its military forces after its defeat in World War I and the humiliating terms of the Treaty of Versailles. Furthermore, the German military leadership had become aware that their pencil-and-paper field cipher, the famous ADFGVX cipher, had been broken by French cryptographers only a few months after its deployment in 1918, leading to at least one significant military defeat for the Germans. In order to prevent a repetition of the ADFGVX debacle, the Germans switched to Enigma as their primary system for secret communications.

The different branches of the German military also employed slightly different models of the Enigma cipher machine. In 1943, the German military deployed the SZ42 cipher machine for use over 26 crucial communications links. The SZ42 employed the stream-cipher technique, in which identical key-streams of pseudorandom characters are generated at both the sending and receiving end of the link and added, character by character, to the individual characters of the plaintext (for ciphering) or ciphertext (for deciphering). The German military did not replace Enigma with the SZ42 for general use because the SZ42's complexity made it too heavy for the field.

The SZ42 cipher proved difficult for allied cryptographers to crack, as did another German cipher machine, the Geheimschreiber, first deployed by the German navy in 1942. However, Allied cryptographers cracked the Enigma, SZ42, and Geheimschreiber ciphers by building specialized devices to systematically try out possible keys





Enigma cipher machines displayed at the National Cryptologic Museum in Fort Meade, Maryland. ©RUBIN STEVEN/CORBIS SYGMA.

for the decryption of messages. The first such devices—“bombes,” invented by Polish mathematician Marian Rejewski (1905–1980) and possibly named for the loud ticking noises they emitted while functioning—were electromechanical (i.e., used a combination of electrical currents and moving parts). Bombes sufficed for the Enigma cipher, but to crack the SZ42 and Geheimschreiber ciphers, the Allies built what is sometimes considered the world’s first electronic computer, the Colossus. The Colossus was based primarily on the ideas of British engineer T. H. Flowers (1905–1998) and British mathematician Alan Turing (1912–1954). (An “electronic” computer, as opposed to an electromechanical device, does not use moving parts to perform its calculations.)

Cipher-machine technology reached its peak in the Geheimschreiber and SZ42 cryptosystems, achieving a level of cryptographic security that could only be breached by the invention of a wholly new technology: the electronic computer. Nevertheless, all the major German ciphers of the World War II—and the primary Japanese cipher too, codenamed Purple—were broken by the Allies.

The Allies also used cipher machines during World War II, but with better luck, as the Axis governments did not succeed in breaking Allied ciphers routinely. The United States Army’s primary cipher machine descended from a

compact device invented by Swedish inventor Boris Hagelin (1892–1983) in the mid 1920s. Hagelin’s cipher machine, originally designated the B-21, sold thousands of copies to the French military between 1934 and the French defeat in World War II. The U.S. Army purchased Hagelin’s machine after the German invasion of Norway in 1940 and redesignated it the M-209. More than 140,000 M-209s were manufactured before the end of the war. The M-209, like the SZ42, employed the stream-cipher technique, with matched generation of the key-stream at the transmitting and receiving ends of each link. Interestingly, this technique is still used today in applications such as digital pay-TV, file encryption, and communication with secure Web sites; however, electronic, rather than mechanical, generation of the pseudorandom key stream is used.

Cipher machines continued to be used by many countries for some years after the end of World War II, but were slowly rendered obsolete by the increasing availability of general-purpose digital computers. The displacement of cipher machines by computers was inevitable for several reasons. A computer can be flexibly reprogrammed to implement any number of ciphering schemes, whereas a cipher machine can implement only the cipher it is built for. Further, electronic computers operate at far higher speeds than can mechanical devices. Today, all serious

ciphering is performed using digital computers, and the only remaining ciphering machines are in museums.

## ■ FURTHER READING:

### BOOKS:

Churchouse, Robert. *Codes and Ciphers*. Cambridge University Press, 2002.

Deavours, Cipher, et al. *Cryptology: Machines, History and Methods*. Norwood, MA: Artech House, 1989.

Singh, Simon. *The Code Book*. New York: Doubleday, 1999.

### SEE ALSO

*ADFGX Cipher*  
*Cipher Pad*  
*Codes and Ciphers*  
*Purple Machine*

---

## Cipher Pad

---

### ■ LARRY GILMAN

A cipher pad is a printed list of cipher keys, each intended to be used for the encipherment and decipherment of a single message. Cipher pads (also termed one-time pads) are closely related to one-time tapes and stream ciphers, which are discussed below.

A key is a string of letters or numbers that is needed to correctly encipher or decipher a message. Each distinct key produces a unique ciphertext from a given plaintext (and vice versa). Both sender and receiver must therefore, know the key associated with a specific message if the message is to be successfully enciphered and deciphered. As long as the key remains unknown to an opponent, the enciphered message is secure. If an opponent, however, does manage to steal or guess the key—for example, by systematically trying out all possible keys—then they will have broken the cipher and can decipher the secret message. Another weakness of ordinary key-based ciphering is that the more text is sent using a single key, the easier it is for an opponent to deduce the key by analysis of intercepted messages.

These facts suggest two basic rules of key use: (1) Change keys often. This prevents an opponent from building up a large mass of text, all enciphered by the same key, which can be used to deduce the key. (2) Use long keys. This makes it impractical for an attacker to find the right key by pure guessing. For example, if the key is a 56-bit binary number (as it is for the Data Encryption Standard, a

U.S.-government-designed ciphering system widely used since 1977), then there are  $2^{56} > 7.2 \times 10^{16}$  possible keys.

A cipher-pad system takes key changing to a logical extreme by using a different key for every message. The keys used are, furthermore, long enough to keep an opponent from simply guessing at them. These selected keys are printed in a book (the cipher pad), the pad is distributed to all senders and receivers, and the keys in the pad are used up one by one as messages are sent. This has the disadvantage that only a limited number of messages can be sent before a new cipher pad must be printed and distributed. Also, as with codebook systems, there is always the danger that a copy of the book will be captured. For these reasons, printed cipher pads have not often been used.

**Principle of ciphering.** The cipher-pad principle is important, however, when combined with the following fundamental principle of ciphering: *A cipher employing a key that is at least as long as the message itself and is never used for any other message can be made truly unbreakable.* This is easy to verify: imagine a message 50 letters long that has been encrypted using a key 50 letters long. To guess the correct key means trying out all possible 50-letter strings. Even if this were practical—and it is not, for there are  $26^{50} > 10^{70}$  such strings, more than the number of atoms in our galaxy—generating all keys 50 characters long is the same thing as generating all messages 50 characters long. Generating all possible messages is the same as simply guessing at what the message is, which is the same as being unable to break the cipher.

The first mechanized application of this principle was the one-time tape system, invented early in the 20th century by U.S. cryptologist Gilbert Vernam (1890–1960) and perfected by Major Joseph Mauborgne of the U.S. Army in 1918. In this system, a message is encrypted as a series of punched holes on a long paper tape. The holes on the message tape are a function of both the message and a randomly generated key (character string) that is as long as the message itself. The key is stored on one tape and the message on the other, and both tapes are shipped by different routes to the intended recipient. The tapes are read simultaneously by a machine that outputs the deciphered text. There is an obvious disadvantage to this technique: the need to send the key. This rules out any kind of telecommunications, for if an enemy intercepted both the key sequence and the message sequence they could decipher the message. Thus, only a perfectly secure transmission channel can be trusted with such information. If the transmission channel is perfectly secure, then there is no need to cipher. The one-tape system is thus, limited to situations in which physical transport of messages is practical.

This limitation is overcome in modern communications by the use of pseudorandom numbers. A truly random number sequence is one that contains no overall

structure or pattern; a pseudorandom number sequence is one that looks like truly random sequence but is in fact produced by a series of arithmetical calculations that can be repeated at will. Pseudorandom number sequences are easy to generate in digital computers using arithmetical procedures termed pseudorandom number generators (PNGs). The bits produced by a PNG can be strung together into a stream that is as long as any desired message. This stream of bits is termed "the cryptographic bit stream" or "key-stream." A message can then be encrypted by performing the EXCLUSIVE OR (XOR) operation pairwise on bits from the message-stream and the key-stream. The XOR operation for two bits is defined as follows:

INPUT 1	INPUT 2	OUTPUT (XOR)
1	1	0
1	0	1
0	1	1
0	0	0

The following is a message-stream, a key-stream, and the encrypted bitstream produced by XORing the message-stream and the key-stream together:

```

Message-stream:  1 0 1 1 0 0 0 1
Key-stream:      0 1 0 1 0 0 1 1
Encrypted bitstream:  1 1 1 0 0 0 1 0
    
```

It is easy to verify that each bit in the encrypted bitstream is the XOR of the two bits above it.

The XOR function is used for encipherment because it has the following useful property: the XOR of the encrypted bitstream and of the key-stream recovers the message-stream.

```

Encrypted bitstream:  1 1 1 0 0 0 1 0
Key-stream:          0 1 0 1 0 0 1 1
Recovered message:   1 0 1 1 0 0 0 1
    
```

In the example above, it is easy to verify that each bit in the recovered message is the XOR of the two bits above

it. Because cipher systems of this type work on streams of bits, they are termed stream ciphers.

The discussion so far assumed that the receiver of the encrypted message has access to the same key-stream as the sender. In a cipher-pad or one-time-tape system, agreement on the key sequence is assured by sending the key (on paper or some other medium) to both ends of the link. In a stream cipher, it is assured by generating the key-stream at both ends of the link. Because the pseudorandom bits of the key-stream are generated by a PNG, both ends of the cipher link need only start their PNGs at the same point in its series of operations to generate the same key-stream. This can be accomplished by transmission to the receiver of a group of numbers termed a "seed" or "initializing vector."

**Quantum cryptography.** Weak points exist even in this system. For example, all PNGs start to repeat themselves eventually, and so do not produce truly random numbers. Also, the initializing vector must be known somehow at both ends of the cipher link. The answer to these difficulties may be resolved using quantum cryptography. In quantum cryptography, stream ciphering returns to the old idea of sending a key-stream along with the message. However, the key-stream is not sent on a paper tape or even as a conventional digital message. It is generated by the sender as a series of truly random subatomic events and shared by the sender and receiver using pairs of "entangled" photons that cannot, by the most fundamental laws of physics as they are now understood, be intercepted without revealing the presence of the eavesdropper.

Real-world quantum-cryptographic systems are being developed rapidly, and proof-of-concept systems have already been built. Thus, there seems to be no basic obstacle to the development of truly unbreakable quantum-cryptographic systems, the ultimate development of the cipher-pad concept.

■ FURTHER READING:

BOOKS:

Meyer, Carl H., and Stephen M. Matyas. *Cryptography: A New Dimension in Computer Data Security*. New York: John Wiley & Sons, 1982.

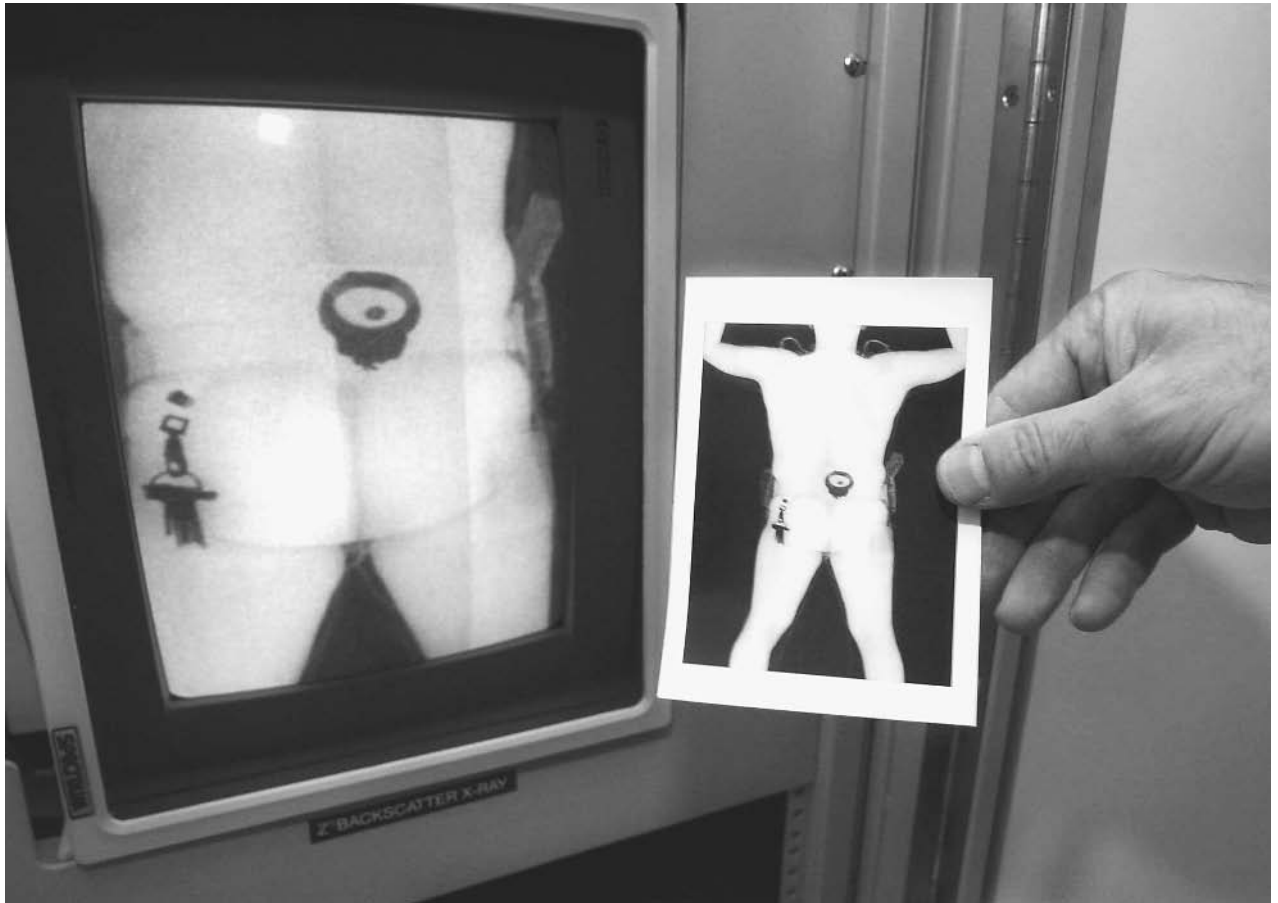
Mollin, Richard A. *An Introduction to Cryptography*. New York: Chapman & Hall, 2001.

PERIODICALS:

Bennett, Charles H., and Peter W. Shor. "Privacy in a Quantum World." *Science* no. 5415 (1999): 747-748.

SEE ALSO

*Codes and Ciphers*  
*Quantum Physics: Applications to Espionage, Intelligence, and Security Issues*



A customs officer inspects a BodySearch image, which uses x-ray technology to allow inspectors to detect contraband on arriving passengers who choose not to submit to the traditional "body pat down." AP/WIDE WORLD PHOTOS.

## Civil Aviation Security, United States

■ JUDSON KNIGHT

Civil aviation security in the United States is directed by the Transportation Security Administration (TSA), which was created after the terrorist attacks of September 11, 2001, under the Aviation and Transportation Security Act (ATSA). Prior to November 19, 2001, when President George W. Bush signed ATSA into law, the Federal Aviation Administration (FAA) handled civil aviation security. The passage of the new law, and the creation of the new administration, required changes to the federal statutes covering aviation security, which are contained in Title 49 of the Code of Federal Regulations, Chapter XII parts 1500 through 1699.

ATSA mandated increases in the numbers of federal air marshals, and placed airport security screeners under

federal control. It required that all screeners be U.S. citizens (a provision later challenged by the American Civil Liberties Union), and that all bags be screened or matched to passengers. It also included provisions for awards of \$1.5 billion to airports and private contractors to meet the direct costs of meeting new security requirements.

The law created TSA, to be headed by a Transportation Department undersecretary for security appointed by the president and confirmed by the Senate. Overseeing TSA would be a new Security Oversight Board consisting of cabinet secretaries, or their designees, from the departments of Transportation, Defense, Treasury, Justice, and Homeland Security (the latter, then the Office of Homeland Security, became a cabinet-level department on March 1, 2003), as well as one representative each from the Central Intelligence Agency and the National Security Council.

The undersecretary would appoint a federal security manager at each airport nationwide, and was authorized to provide air marshals as he or she saw fit. Each flight deemed a high security risk would have air marshals, who could be appointed at the undersecretary's discretion. In consultation with airport and law enforcement officials,

the undersecretary would order the safeguarding of airport areas as needed.

In the field of airport security screeners, these were placed under federal control as uniformed TSA employees. Airport security screeners had to be proficient in English, pass background checks, undergo a minimum of 40 hours' classroom instruction or the equivalent, complete 60 hours on-the-job training, and be tested each year.

In addition, the undersecretary was authorized to establish a test program whereby five airports (one from each of five levels of security risk) would be permitted to contract directly with private companies. These companies would have to have standards at least as high as those of the federalized screening force, which would operate at all other hub airports—of which there were 424 total in the United States at the time—for two years. At the end of two years, airports would be allowed to opt out of the federalized screening program if they so choose.

Within 60 days, all checked baggage would have to be screened, either by explosives detection machinery, or manually. The law also authorized the Secretary of Transportation to require airports to use all necessary equipment for the detection of chemical or biological weapons.

■ FURTHER READING:

PERIODICALS

- Croft, John. "Air Security Bill Clears Lawmakers' Logjam." *Aviation Week & Space Technology* 155, no. 21 (November 19, 2001): 46.
- "Responses to ASR's Survey on Aviation Security Post-Sept. 11." *Airport Security Report* 9, no. 19 (September 11, 2002): 1.
- "S. 1447, Aviation and Transportation Security Act." *Airports* 18, no. 48 (November 27, 2001): 5.

ELECTRONIC

Transportation Security Administration. <<http://www.tsa.gov/public/>> (March 5, 2003).

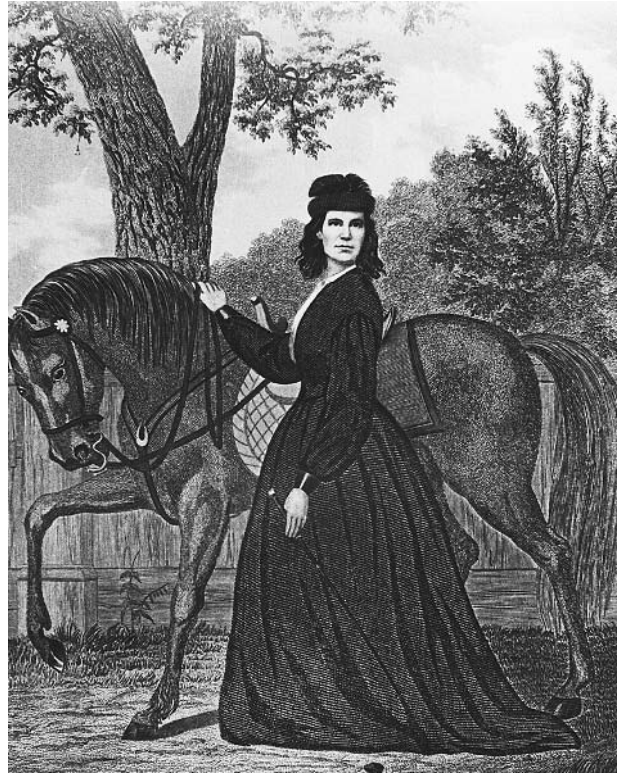
SEE ALSO

- Air marshals, United States*
- Aviation Security Screeners, United States*
- FAA (United States Federal Aviation Administration)*
- September 11 Terrorist Attacks on the United States*
- Transportation Department, United States*

## Civil War, Espionage and Intelligence

■ WILLIAM J. ENGLE

During the great American conflict of the middle nineteenth century, the Civil War, efforts by both the North and



Portrait of Emma Edmonds, famous woman spy of the Civil War. ©BETTMANN/CORBIS.

South to engage in espionage and intelligence-gathering activities were unparalleled in the history of the relatively young nation. Although daring, these efforts were often quite amateurish by modern standards.

The physical environment of America greatly facilitated covert activities. With America as the "melting pot" of the world, people throughout the nation represented every race and nationality in the world. Unionist and secessionist alike came from every corner of the country and both sides consisted of people of every race, creed, and color. Visually, covert combatants could not be easily identified one from another. Americanized English was the common language, but even with many regional dialects, there were few specific speech patterns unique to either side. State or region of origin was no guaranty of which side one might take in the conflict.

People were free to travel practically at will. Boundaries between Union and the Confederate held areas existed primarily as lines on a map and posed no controlled barrier to travel. Many major rivers traversed the land north to south. Major mountain ranges trended north/south. Railroads and roadways had been developed in all directions. Getting to and from one area to another was relatively easy and borders were difficult to control. Spies and agents were free to roam practically at will restricted more by their own skill and courage than any other factor.

With travel being relatively unimpeded it was fairly easy to pass written or memorized verbal messages through the lines. Both sides developed methods to encrypt messages using various forms of alphanumeric sequence codes and cipher wheels. The telegraph was the leading communication technology of the period. Anyone with a portable key set could tap into any line and monitor, receive, and send messages often confusing and countermanding orders being sent over the wire. Confederate cavalry leader John Hunt Morgan habitually included a telegraph operator on his staff just for this purpose. Hunt was so daring as to send a message to the U.S. Commissary Department over telegraph lines operated by the U.S. Army complaining about the quality of mules being supplied to units opposing him and being captured by his men. Requisitions for supplies were often submitted in similar fashion in anticipation of capture from the adversary.

Hot air balloons were introduced by both sides for observing troop movement and disposition, spotting artillery fire and relaying signals.

The Confederacy led in the development of “infernal weapons” such as mines and torpedoes that were, at the time, considered violations of the rules of war as they acted upon unsuspecting prey. The concept of these devices was relatively simple in including a black powder charge within a watertight container and a detonation device. The Brooke buoyant torpedo consisted of a metal dome with contact detonators on top mounted on a metal conical shaped container attached to a wooden spar anchored on the bottom of a waterway. At times a Turtle torpedo containing as much as 100 pounds of explosives would be attached by wire to the base of the spar. Attempts to remove the adjacent buoyant torpedo would pull the wire and detonate the Turtle. Other torpedo designs included floating containers detonated by contact or electrical charge from a shore based agent and free floating drifting mine detonated by an attached propeller mechanism after coming to rest against the hull of a ship. River and sea torpedoes could be placed by agents or troops in advance of the arrival of the opposing force.

However, the Coal torpedo required placement in a fuel storage depot or bunker by an agent and quite often in the presence of the enemy. The Coal torpedo was made of a hollow chunk of iron cast to look like a piece of coal. The fake coal contained a charge of powder and was coated with tar and coal dust and exploded with tremendous effect when fed into the boiler fire of a steam engine either on board a ship, on a train or in a factory.

Agents on the ground were the backbone of the espionage and intelligence gathering efforts of the period. Unfortunately the identity of most of the agents of the conflict was lost as many operated under multiple names; records were often poorly kept, and lost or intentionally suppressed or destroyed. Contraband and escaped slaves served as a primary source of intelligence for the U.S.

Army. However, a former barrel maker, sheriff and native of Scotland organized a detective agency in 1850 that served the Union effort extensively and is still in business today. Alan Pinkerton formed the National Detective Agency and gained fame by foiling a plot to assassinate President Lincoln in 1861 and went on to create the secret service of the U.S. Army. Neither Pinkerton nor his agents had any training in intelligence gathering and were notorious for their tactics and the over-estimation of Confederate troop strength. During the Peninsula Campaign over the spring and summer of 1862, General G. B. McClellan (U.S.) had advanced the Army of the Potomac and its 108,000 effectives to within sight of the church spires of the Confederate capital city—Richmond, VA. However, based on intelligence gathered by Pinkerton that suggested a potential opposing Confederate force nearing 200,000 who were well fortified with reinforcements en route, the general paused to plead his case with Lincoln for more troops. In fact, General R. E. Lee never had more than 85,000 effectives under his command during this time, as his smaller force drove the Federal horde before him in full retreat. Pinkerton’s unintended misinformation may well have served the defense of the Confederate capital city better than the mythical reinforcements that were not coming. It would be some two and a half years before the U.S. Army would get that close to Richmond again. Yet, Pinkerton and his organization remained in Federal service well beyond the war. Much of Pinkerton’s information came from criminals and escaped slaves who lacked the skills of espionage and were thus, prone to exaggeration, along with agents who may have spent more time enjoying Richmond’s pleasures than actually counting troops in the field. In time, the Confederates learned to appreciate the value of misinformation and intentionally sent men forward to become captives of the Federal forces and spread inaccurate information.

American culture was still quite Victorian in many ways during the 1860’s. Women agents had a decided advantage over their male counterparts, as they were not likely to be as roughly interrogated or possibly executed upon discovery. Both sides took full advantage of the opportunity.

Belle Boyd shot and killed one of two drunken Union soldiers who had entered her Martinsburg, VA home on July 4, 1861. She was acquitted and set free. Thereafter, Boyd voluntarily forwarded her written observations of Union activity in her area to local Confederate authorities. During General “Stonewall” Jackson’s Shenandoah Valley Campaign, Union troops occupied the town of Front Royal, VA where Miss Boyd happened to be at the time. Observing the panic that developed among the invading Federals upon their learning of Jackson’s approach and overhearing their plans to burn a large supply depot in town and the bridges across the South Fork of the Shenandoah River as they retreated northward, seventeen year old Belle decided to inform the Confederate forces personally. Under fire from Union pickets, Boyd dashed several

miles to carry her knowledge to the approaching Confederate column. The leading elements of the column then dashed forward to save the bridges that later enabled Jackson to drive up the valley driving the forces of Union General Nathaniel Banks before him and freeing the vital area's food supply to Confederate purpose.

Belle Boyd continued her activities until arrested on July 29, 1862, and was transferred to the Old Capital Prison in Washington, D.C. No charges were pressed and she was released one month later, where upon she returned to Richmond and continued her work as a spy. Later she was arrested aboard the blockade runner *Greyhound* outbound for England but managed to persuade Federal Lieutenant Harding, who had been placed as prize master of the captured ship, to permit Confederate Captain Lewis to escape en route to Boston. Before the end of the war, Miss Boyd and Lt. Harding married.

Elizabeth Van Lew, a native of Richmond, VA who had attended a Philadelphia Quaker school, was an ardent opponent of slavery and pro-Union. After the war broke out, Van Lew was granted permission to care for Union prisoners. Many of the prisoners had observations of Confederate positions and troop dispositions that they hoped to get back to Union authorities. Miss Van Lew established a network of couriers, developed a secret code, and began passing messages through the lines to Union forces. Many in Richmond referred to her as "Crazy Bet" as she hummed and mumbled to herself as she traveled the town, while believing her sympathy for the Union was part of her mental illness. "Crazy Bet" is credited with procuring for Mary Elizabeth Bowser, a former slave whom she had freed before the war, a job as a house servant in the home of Confederate President Jefferson Davis. Together, the two women collected valuable information that was passed on to Union officers. "Crazy Bet" managed to maintain her cover throughout the war and was one of the first people to be visited by General U.S. Grant upon the taking of Richmond. Later, President Grant appointed her postmaster of Richmond though the people of the city shunned her once they realized the harm she had rendered to the Confederate cause.

Emma Edmonds, who was able to join a Michigan volunteer company by posing as a man, gathered information for her company by "posing" as a woman.

Legends and folklore are rich with stories of individual daring and accomplishment as agents and double agents during the Civil War, but verifiable documentation is only available in a few cases. Some of the best intelligence gathering opportunities came about as random luck. Perhaps one of the most significant instances of pure luck delivering critical information into the hands of the enemy was the discovery of a copy of General R. E. Lee's order of march as he moved northward in September of 1862. A note was found on the ground wrapped around three cigars by Federal soldiers that contained details of the order of march of General R. E. Lee's divided forces

marching through the Shenandoah Valley on their way to carry the war to the North on their home ground. Some historians assume that a member of General D. H. Hill's subordinate command dropped this bit of critical information. Union General G. B. McClellan had been cautiously seeking the Confederate force, and the discovery of General Lee's order of march enabled McClellan to unexpectedly close on them and force an unplanned battle near Sharpsburg, MD along Antietam Creek. The battle unfolded to become the most deadly single day of combat in American history, and ended in a tactical victory for the South in that its army escaped annihilation and withdrew southward in good order after Union forces refused to attack the following day. However, the North claimed a major strategic victory that changed the nature of the war, and ended consideration of European intervention on the side of the South.

Both the Union and the Confederacy had agents working throughout the territory of the other. The Northern media proved to be of great aid to the Southern intelligence gathering effort. Northern papers continually ran articles describing current events, Union troop dispositions, and future movement in such detail that undercover Confederate agents kept a constant supply of daily newspapers heading south from major cities such as New York, Philadelphia, and Boston to commanders in the field.

Spying was not limited only to opponents. There was considerable spying by various political factions on their own battlefield commanders and faction against faction. This was particularly true on the Union side where trust between President Lincoln, the cabinet, prominent congressmen, and the military staff was particularly low during the early years of the war, as the search for a commander who could defeat the secessionists created considerable turmoil. Many Federal commanders also dreaded the political opponents in their rear as much as the combat opponents to their front, as many officers were removed to satisfy public whim.

#### ■ FURTHER READING :

##### BOOKS:

- Coggins, Jack. *Arms and Equipment of the Civil War*. Wilmington, NC: Broadfoot Publishing Company, 1990.
- Canton, Bruce. *The Civil War*. New York: American Heritage/Wings Books, 1960.
- Foote, Shelby. *The Civil War—A Narrative*. New York: Vintage Books/Random House, 1986.
- Stern, Philip Van Doren. *Secret Missions of the Civil War*. New York: Wings Books, 1990.

##### ELECTRONIC:

- University of Virginia, "Hearts at Home: Spies <<http://www.lib.virginia.edu/speccol/exhibits/hearts/spies.html>>(March 22, 2003).



Alberta Lee, daughter of Los Alamos scientist Dr. Wen Ho Lee, protests her father's imprisonment outside the Federal Building in San Francisco. Lee was arrested in 2000 for mishandling classified information. AP/WIDE WORLD PHOTOS.

## Classified Information

■ JUDSON KNIGHT

Classified information is any data or material that belong to the federal government and relate to sensitive topics such as military plans or the vulnerabilities of security systems. A number of laws or rules govern the control of classified information and access thereto, as well as the declassification of items no longer sensitive. Thanks to Executive Order 12958, a number of formerly classified documents regarding the Cold War and other critical junctures in U.S. security history are now accessible to the general public.

As defined in the Classified Information Procedures Act (CIPA), passed by Congress in 1980, classified information is any information or material that has been determined by the United States government pursuant to an

executive order, statute, or regulation, to require protection against unauthorized disclosure for reasons of national security and any restricted data, as defined in paragraph R of section 11 of the Atomic Energy Act of 1954 (42 U.S.C. 2014[y])

The act names executive orders before legal statutes, because these orders—more than acts of Congress, decisions of the Supreme Court, or other rulings—are among the principal governing authorities in matters of security classification and access to classified information. In addition to executive orders, there are also other non-parliamentary government directives that present guidelines on classified information and access.

For the present purposes, it is helpful to be a bit more explicit than CIPA, and—using as a basis various executive orders, as well as historical practice—define classified information as materials or data belonging to, controlled by, and/or produced by the federal government, pertaining to intelligence sources or methods of collecting information; cryptology or codes; and the vulnerabilities, capabilities, or planning of systems, installations, or projects that relate to national security. Access to information thus “classified” is restricted on the basis of its relative importance, the consequences that would follow if it were passed to the wrong parties, and the individual’s “need to know” that information.

**Laws on classification procedures: An introduction.** Federal laws on classification procedures provide for governing authorities who determine what information should be subjected to rules of restricted access. Specifically, Executive Order 12958, discussed below, defines the “original classification authority” as “an individual authorized in writing, either by the President, or by agency heads or other officials designated by the President, to classify information in the first instance.” This governing authority also determines the level of classification, of which are three major ones: confidential, secret, and top secret. (The levels of security clearance are discussed in more detail elsewhere, within the context of security clearance investigations.)

A number of laws govern classified information, but most are not “laws” in the sense that they were duly reviewed by Congress or the Supreme Court; rather, the majority of guidelines in these matters come from executive orders or presidential directives (which are classified), as well as directives from the National Security Council, the director of Central Intelligence, the Department of Defense, and so on. A rare exception to this is CIPA, the Classified Information Act, which came into being through the ordinary channels of legislative procedure most commonly associated with a republican democracy. Even so, it has often been used to protect the “shadow government” of the security and espionage apparatus.

**Classified Information Act (CIPA).** Passed by Congress on October 15, 1980, CIPA was codified as 94 Stat. 2025, 18





Speaker of the House of Representatives Dennis Hastert listens as Senate Majority leader Tom Daschle talks with reporters in October 2001, about Congressional leaks of classified information. AP/WIDE WORLD PHOTOS.

U.S.C. Appendix, and further amended November 18, 1988, in 102 Stat. 4396. Known in legal circles as a procedural statute, CIPA presents guidelines for the use of classified information by both government and defendant in a legal case. As a procedural statute, it neither adds to nor subtracts from the rights of the defendant or the obligations of the government; rather, it is designed to prevent both sides from unauthorized disclosure of classified information, and to apprise the federal government of any security breach that may result from proceeding with a case.

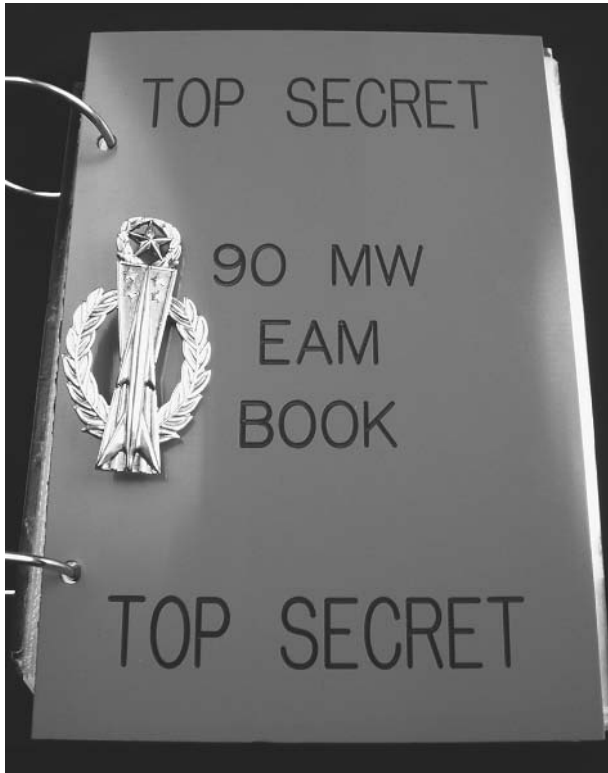
During the Iran-Contra conspiracy trials in 1988, attorneys representing defendants Oliver North, John Poindexter, Richard Secord, and Albert Hakim filed a petition with U.S. District Judge Gerhard A. Gesell, stating that CIPA “imposes burdens on the defense unprecedented in American law.” Because so much of their case rested on classified information, the defense argued, it would be legal suicide to disclose all of that information to the prosecution.

CIPA continued to be a theme throughout the proceedings. In July 1989, North’s attorneys filed an appeal

stating that Gesell, who established guidelines for compliance with CIPA, nevertheless permitted infringement of North’s constitutional rights. Later, Senate majority leader George Mitchell complained that CIPA was too lenient, because it allowed Thornburgh to put a stop to the trial of Costa Rica Central Intelligence Agency (CIA) station chief Joseph F. Fernandez for his role in Iran-Contra.

More than a decade after Iran-Contra, attorneys representing Chinese scientist Wen Ho Lee, accused of stealing secrets from the Los Alamos National Laboratory, attempted to use CIPA in a way different from that of North or Poindexter. Instead of withholding information, they were convinced that the release of highly sensitive data that the government had no desire to reveal publicly was a major reason for the government to avoid vigorous prosecution of Lee on the most serious charges.

**Executive Order 12958.** The most significant presidential provisions regarding classified information are the executive orders 12958 and 12968, both issued by President William J. Clinton. The second of these is discussed elsewhere, in the context of security clearances. The first,



A top-secret procedure manual used for instructing military officers in the event of a nuclear missile launch rests on a desk at the Warren Air Force Base missile launch complex. ©JAMES A. SUGAR/CORBIS

titled "Classified National Security Information," was signed on April 17, 1995. According to its opening sentence, the order "prescribes a uniform system for classifying, safeguarding, and declassifying national security information."

In addition to defining "classification" and the basic levels thereof, as well as types of information that may be classified, the order provides that "If there is significant doubt about the need to classify information, it shall not be classified." Furthermore, "If there is significant doubt about the appropriate level of classification, it shall be classified at the lower level." The order prescribes the use of classification markings to distinguish varieties of classified information, and provides for "derivative classification," or "the incorporating, paraphrasing, restating or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information."

**Declassification and Executive Order 13142.** Particularly important are the provisions of Executive Order 12958 with regard to declassification, or the removal of restrictions on access to information. Declassification is not to be automatic, "as a result of unauthorized disclosure of identical or similar information." However, except in specific

circumstances, information is to be automatically declassified after 10 years. Those specific circumstances include situations in which national security would be jeopardized by disclosure of the information, as well as instances in which automatic declassification could violate a legal statute. A notable example of such a statute is the Privacy Act of 1974.

Executive Order 13142, signed November 19, 1999, amended 12958 by extending the amount of time until certain types of information can be declassified. Specifically, the order addresses Section 3.4 in the earlier order, which provides for the declassification of information more than 25 years old that has been determined to have historical value in accordance with Title 44, U.S. Code. Whereas the earlier order had provided for declassification within five years, 13142 extended this period for 18 months. As the *Washington Times* reported in December 1999, this change angered the American Legion and other veterans' groups eager to search records from the Vietnam era for information regarding prisoners of war (POWs) and others who were missing in action (MIAs).

**Post-12958 declassification efforts.** An August 1998 White House press release called Executive Order 12958 became "the first effort since the end of the Cold War to reassess the balance between open government and the need to maintain secrets vital to national security." Although critics disputed White House claims as to the extent of the effort, the order did open a vast body of information for declassification. According to the press release, the Interagency Security Classification Appeals Panel established by the order had, in the three years that followed its issuance, reviewed some 96 documents and released 81 of them.

Among these were documents from the administrations of presidents Dwight D. Eisenhower, John F. Kennedy, and Lyndon B. Johnson regarding the deployment and possible use of nuclear weapons in Europe; two 1962 letters from Indian Prime Minister Jawaharlal Nehru to Kennedy expressing fears of an impending nuclear war between his nation and China; State Department communications regarding Israeli nuclear capabilities during the June 1967 Six-Day War; and a September 1967 memorandum to Johnson regarding military options available to the North Vietnamese army. Less than 25 years old were documents from the administration of President Gerald R. Ford concerning nuclear weapons programs in South Korea. Some of the latter information remained classified, because disclosure would endanger a source, or because its release would harm U.S. relations with foreign governments.

**NSA and NIMA records.** The National Security Agency (NSA) subsequently undertook a review of documents for declassification, a project it named OPENDOOR. As NSA announced in a press release dated April 2, 1996, it had

turned over some 1.3 million pages of declassified documents to the National Archives and Records Administration (NARA). Intriguing as the contents were, these documents were far more than 25 years old; rather, they dated from the beginning of World War I to the end of World War II. Among them were a cryptologic study of the 1917 Zimmermann telegram that precipitated U.S. entry into World War I; information on the Native American "Codetalkers" of World War II; and the captured diary of a Nazi U-boat.

Much more recent were the photographs released by the National Imagery and Mapping Agency (NIMA) in 1996 and again in 2002. These included millions of frames of imagery taken by KH-1 through KH-6 spacecraft, the KH-7 Surveillance Imaging System, and the KH-9 Geospatial Imaging System. Taken between 1963 and 1980, the images from the "Keyhole" satellites included shots of Hanoi and Beijing, Egypt's Aswan Dam, the Eiffel Tower, and the U.S. Capitol building. Still withheld were numerous images, some dating as far back as 1963, that were still considered too sensitive for release.

**NARA, CIA, and the Continuing Task of Declassification.** Further information regarding documents released in accordance with Executive Order 12958 is available at the NARA Web site. With the help of teams sent by CIA under a project known as "Remote Archives Capture Project," NARA had by the early twenty-first century declassified millions of pages of material. Among these were State Department files offering information on Nazi gold from World War II; Kennedy's tapes of conversations during the Cuban missile crisis of October 1962; the January 1968 incident in which sailors from the U.S.S. *Pueblo* were captured by North Korea; headquarters reports from U.S. military commands in Vietnam and Thailand through 1975; information on POWs and MIAs from Korea and Vietnam; and records of U.S. participation in SALT (Strategic Arms Limitation Talks) negotiations.

It was an intriguing collection, but much remained to be processed by historians, scholars and archivists. Some of the processed information may remain classified indefinitely. According to Michael J. Kurtz, aside from "unique items such as Secret Service records relating to the protection of the President and Internal Revenue Service tax information," items exempted from release fell into four basic groups: information on atomic energy; intelligence sources and methods; sensitive foreign-relations topics (e.g., U.S. discussions on border disputes between other nations, such as that between India and Pakistan over Kashmir); and information from foreign governments that the latter had not approved for release.

#### ■ FURTHER READING:

##### BOOKS:

*Disclosure of Classified Information to Congress.* Washington, D.C.: U.S. Government Printing Office, 1998.

Richelson, Jeffrey T. *The U.S. Intelligence Community*, third edition. Boulder, CO: Westview Press, 1995.

##### PERIODICALS:

- Black, Chris. "Mitchell Urges New Classified Data Law." *Boston Globe*. (December 5, 1989): 3.
- Elvin, John. "We've Waited Long Enough." *Washington Times*. (December 27, 1999): 26.
- Lardner, George, Jr. "Classified Trial-Data Law Attacked." *Washington Post*. (April 30, 1988): A4.

##### ELECTRONIC:

- Declassification and Freedom of Information Act (FOIA). Defense Prisoner of War/Missing Personnel Office. <<http://www.dtic.mil/dpmo/foia/>> (January 21, 2003).
- OPENDOOR. National Security Agency. <<http://www.nsa.gov/programs/opendoor/>> (January 21, 2003).
- U.S. National Archives and Records Administration. <<http://www.archives.gov>> (January 21, 2003).

##### SEE ALSO

- Clinton Administration (1993–2001), United States National Security Policy*  
*Executive Orders and Presidential Directives*  
*Iran-Contra Affair*  
*National Archives and Records Administration (NARA), United States*  
*NIMA (National Imagery and Mapping Agency)*  
*Security Clearance Investigations*

---

## Clinton Administration (1993–2001), United States National Security Policy

---

■ CARYN E. NEUMANN

President William Jefferson (Bill) Clinton argued that the end of the Cold War did not mean that the United States could abandon its long-standing aim of ensuring national security by promoting democratization around the world. Now the sole surviving superpower, the U.S. in the 1990s would continue to assertively support democracy but not in a manner that might place American troops in great jeopardy. Fearful of becoming stuck in a Vietnam-like quagmire, the Clinton administration would employ force as a tool of coercive diplomacy and punishment but avoid full-scale conflict. The national security system, re-designed by the new president, would also de-emphasize military issues in favor of a greater emphasis upon economics in the formulation of policy.

President Clinton entered the White House in 1993 with little experience or enthusiasm for international affairs. The first president to take office after the end of the Cold War, President Clinton was also the first to come of



President Bill Clinton, at the head of the table, meets with national security advisors at the White House in November 1995, to discuss the peace agreement in Bosnia. AP/WIDE WORLD PHOTOS.

age during the Vietnam War and he saw national security through the prism of that conflict. Vietnam shaped the Clinton administration in two ways: it made the president reluctant to commit troops to combat and it damaged his standing with the military because he had not served in the military during the conflict. The relative worldwide calm after the dissolution of the Warsaw Pact and the American triumph in the Persian Gulf War made the marginalization of overseas issues politically possible.

As his first national security measure, Clinton issued a presidential directive to revise and rename the framework governing the work of the National Security Council. The previous Bush administration's National Security Review (NSR) and National Security Directive (NSD) series were abolished in favor of a Presidential Review Directive (PRD). The administration would use PRD to re-evaluate security classifications and the safeguarding of systems to ensure that they were in line with the reality of the current dangers instead of the threat potential that had existed during the Cold War.

The second presidential directive (PRD-2) established a new NSC structure, with a broader emphasis on economic issues than in previous administrations. PRD-2 also

established three levels of deliberative committees under the NSC: a principals committee of main NSC meetings, a deputies committee including deputy chiefs of key agencies, and working groups on a variety of issues. Warren Christopher served as Secretary of State, with Anthony Lake heading the NSC until his replacement by his deputy Samuel R. "Sandy" Berger in 1997.

The Clinton administration argued that the end of the Cold War permitted the U.S. to shift to a foreign policy that rested on support for such values as democracy, market economics, humanitarian relief, and genocide suppression. PRD-20 had recommended this overhaul of U.S. policies after concluding that foreign aid programs were often wasteful, incoherent, and inconsistent with U.S. objectives. The most urgent issues that the NSC dealt with in the first years of the Clinton administration were Bosnia (genocide suppression), Haiti (democracy and humanitarian relief), Iraq (strategic arms control), and Somalia (humanitarian relief). Most of the PRDs remain classified, but it is known that the NSC system also dealt with illegal drugs, United Nations peacekeeping, and global environmental affairs.

As Clinton settled into the presidency, he experienced increasing conflict with Congress and a public angered by his policies. A 1993 PRD to permit U.S. forces to operate under the control of a United Nations commander particularly enraged many conservatives and had to be abandoned. The administration responded to its critics by making overseas actions more modest in scope. In Clinton's second term, the administration sought to integrate Eastern and Western Europe without provoking tensions with Russia; to promote more open trade; to improve defenses against such transnational threats as terrorism and narcotics; and to encourage a strong and stable Asian-Pacific community by seeking trade cooperation with China while avoiding confrontation with it on human rights issues.

Critics of administration argue that it appeared to lack a clear consensus on what constituted vital national interests. The obvious reluctance of the president to risk significant numbers of troops to achieve declared political objectives prompted U.S. allies to express concern about reduced American global military involvement and may have encouraged continued troubles with "rogue" nations such as Iraq.

#### ■ FURTHER READING:

##### BOOKS:

Drew, Elizabeth. *On the Edge: The Clinton Presidency*. New York: Simon & Schuster, 1994.

Herrnson, Paul S., and Dilys M. Hill, eds. *The Clinton Presidency: The First Term, 1992–96*. New York: St. Martin's Press, 1999.

##### ELECTRONIC:

Digital National Security Archive. "Presidential Directives on National Security from Truman to Clinton." 2003. <<http://nsarchive.chadwyck.com/pdessayx.htm>>(April 25, 2003).

White House. "History of the National Security Council, 1947–1997." <<http://www.whitehouse.gov/nsc/history.html>>(April 25, 2003).

##### SEE ALSO

*Cold War (1972–1989): The Collapse of the Soviet Union Executive Orders and Presidential Directives*  
*Iraq War: Prelude to War (The International Debate Over the Use and Effectiveness of Weapons Inspections)*  
*Iraqi Freedom, Operation (2003 War Against Iraq)*  
*National Security Advisor, United States*  
*National Security Strategy, United States*  
*NATO (North Atlantic Treaty Organization)*  
*NSC (National Security Council)*  
*NSC (National Security Council), History*

## Clipper Chip

In 1993, officials in the administration of President William Jefferson Clinton announced the proposed use of a cryptographic device intended to protect private communications for all but authorized monitoring by government agencies. Termed the "clipper chip," the device would permit secure encrypted voice communications, but would also allow United States law enforcement and intelligence agencies to monitor those communications by obtaining the algorithm keys to decrypt the transmissions.

As initially proposed the government would allow the keys to be maintained in a database held by an independent agent. Access to those keys would be permitted only as "legally authorized." Critics and privacy advocates immediately questioned the vague and broad use of the term legally authorized."

A chip similar in design and performance specifications, the Capstone chip, could be similarly regulated to allow secure data transmissions that could also be easily decrypted by United States law and intelligence agencies via known algorithmic keys.

An algorithm defines a repeatable step-by-step series of mathematical or language manipulation procedures to encrypt or decrypt a message or communication. Cryptology systems utilize algorithms and the labels, mechanics, recursive procedures, or other solutions are termed "keys" to the algorithm.

Use of the clipper chip was adopted and authorized in 1994. The National Institute of Standards and Technology (NIST) and the Department of the Treasury were designated to be the database repositories or "escrow" agents for the algorithmic keys. Rules regarding access to the keys were developed in accord with state and national security wiretap orders.

The clipper chip utilizes the SKIPJACK algorithm as part of the Escrowed Encryption Standard (EES) program. SKIPJACK was developed as a classified algorithm by the National Security Agency (NSA). SKIPJACK was initially developed as part of the Fortezza encryption suite and is a symmetric cipher with a fixed key length of 80 bits. Security experts assert that multiple encryption programs may eventually replace SKIPJACK like encryption-decryption programs.

#### ■ FURTHER READING:

##### PERIODICALS:

Baker, Stewart A. "Don't Worry, Be Happy: Why Clipper Is Good for You." *Wired*. June 1994.

Johnson, George. "The Spies' Code and How It Broke," *New York Times, Week in Review*. July 16, 1995.

##### SEE ALSO

*Cipher Key*

*Cipher Machines  
Cryptology and Number Theory  
Cryptology, History  
NIST (United States National Institute of Standards and  
Technology)  
NIST Computer Security Division, United States*

## Closed-Circuit Television (CCTV)

■ LARRY GILMAN

Closed-circuit television (CCTV) involves the use of video cameras to produce images for display on a limited number of screens connected directly to a non-broadcast transmission system (e.g., a network of cables). Commercial cable TV is, technically, an example of CCTV, but the term “closed-circuit TV” is generally reserved for systems serving a small number of screens that are monitored for security purposes. CCTV is a ubiquitous feature of institutional security systems. It is employed by prisons, banks, urban police forces, airports, military organizations, utilities, large corporations, various other organizations, and wealthy individuals. Some specific applications of CCTV are:

- X-ray baggage-inspection devices at airports.
- Remote viewing of dangerous industrial processes, rocket liftoffs, and other operations.
- Perimeter security around power plants, military installations, warehouses, police stations, and other defended facilities.
- Intrusion or theft monitoring of secure spaces, whether indoors (halls, lobbies, specific doors and rooms, etc.) or outdoors (parking lots, automatic teller machines, loading docks, etc.).
- Monitoring of vehicular traffic for traffic-control purposes or detection of illegal activity (speeding, smuggling, etc.).
- Identity-checking of persons desiring entry into a building.
- Computerized recognition of individual faces, with possible identification of “wanted” persons.

Two of the most important CCTV applications are discussed in more detail below.

**Perimeter security.** Prior to CCTV, in order to secure the perimeter of an area, it was necessary to post guards in such a way that their lines of sight covered the entire circumference of the area. With CCTV, it is possible to reduce the number of personnel needed to secure a perimeter by placing TV cameras at strategic points and transmitting the resulting images to a control room where a few guards can monitor many screens. Ideally, these

observers will note any suspicious event on their screens and alert a response team. CCTV has thus for decades been a component of the typical Perimeter Intrusion Detection System (PIDS), which combines CCTV with devices designed to detect intrusion by other means (ultrasonic movement detectors, window alarm-contacts, etc.).

CCTV technology, however, has not proved as effective in PIDS applications as was once hoped. As vigilance studies by psychologists confirm, guards who spend hours “screen gazing” at static scenes (> 20 minutes, in tests) tend to become bored and less efficient, and are then likely to miss low-frequency events, such as a figure running up to and climbing over a fence. In the words of Geoff Thiel, a British CCTV-security expert, “Contrary to popular belief, impressive control rooms with large banks of monitors generally do not provide an effective “real time” surveillance service. The vast majority of installed CCTV cameras remain unwatched and incidents are not likely to be detected while they are occurring. CCTV is therefore reduced to a “post-mortem” tool. . .” (1999 International Carnahan Conference on Security Technology).

Starting in the 1980s, designers sought to combat the bored-guard effect by using automatic Video Motion Detectors (VMDs). These devices are designed to automatically detect scene action by comparing successive image-frames for changes. When change is detected that exceeds a predetermined threshold, an alarm is sounded. A guard then judges whether the alarm is false or valid.

VMDs, however, have not turned out to be a security panacea. There are too many sources of image change, especially in outdoor scenes, for a simple circuit to distinguish meaningful intrusions from nuisance alarms: shifting shadows, wind-shaken foliage, birds, rodents, blowing trash or leaves, camera movement, camera auto-iris adjustments, and the like. Faced with frequent false VMD alarms, guards tend to ignore the system altogether. VMD use is therefore restricted to artificially-lighted indoor spaces or to expensive systems that employ computer processing to reduce the false-alarm rate.

In the 1990s and beyond, artificial intelligence techniques—in particular, expert systems—have been combined with VMD to increase the effectiveness of CCTV. An expert system applies higher-level processing to information extracted from the pixels of the raw CCTV image in order to identify and track objects, usually including human intruders. Such systems are a definite improvement over simplistic VMD, and have proven their potential to ignore waving tree-limbs and rabbits hopping over lawns. However, progress remains slow, as in all artificial-intelligence efforts to navigate uncontrolled, complex, real-world situations. A large number of explicit classification rules, for example, must be generated to enable a program to “understand” a given scene—and a scene may change its appearance radically depending on weather (e.g., fog, snowfall, rain), time of day, number and type of cars in the parking lot, and numerous similar factors. It is,



Nikolay Volodiev Dzhonev, center, appears on a television monitor during his closed-circuit arraignment in 2002 after he was arrested for attempting to board an airplane en route from Atlantic City, New Jersey to Myrtle Beach, South Carolina, with box cutters and a pair of scissors in his backpack. AP/WIDE WORLD PHOTOS.

therefore, difficult to make a PIDS expert system expert enough to be authentically useful. PIDS designers continue to emphasize that there is no near prospect of intelligent CCTV systems outperforming human guards, with all their weaknesses.

**Public-surveillance CCTV.** Surveillance by police of sidewalks, train stations, courtyards, parking lots, and other public spaces has proliferated rapidly throughout Europe and the United States during the last decade, propelled largely by the increased availability of inexpensive electronics. Many major cities, including Copenhagen, London, New York, and Washington, D.C., now possess public-surveillance CCTV systems, most often operated by police departments. In some cases, images from these systems are being processed using facial recognition systems (also termed biometric systems, from the Greek for “life measurement”). Facial recognition systems are software algorithms that seek to extract telltale facial features from video images and match faces in photographs to those in a database. Public-surveillance systems are thus

advertised as serving two basic purposes, deterrence of crime in watched areas and identification of wanted persons.

Such systems have been criticized on several grounds. In Britain, where public-surveillance CCTV has been in use since the 1980s, studies have cast doubt on whether CCTV has any tendency to reduce crime through deterrence. Crime sometimes decreases in monitored areas, but many criminologists argue that this is because criminals simply move their activities elsewhere. Further, facial-recognition software has an extremely low success rate. Several systems, including ones deployed by the city of Tampa, Florida and by the U.S. Immigration and Naturalization Service, have been abandoned within months of deployment due to their zero or near-zero success rates. Police databases have also occasionally been used by individuals with access for illegal purposes (e.g., stalking ex-spouses, blackmailing), and public-surveillance CCTV systems, like any powerful surveillance tool, are vulnerable to such abuse. Further, system operators, who are usually male, sometimes use CCTV systems to voyeuristically

observe women; a British study found that 1 in 10 women were targeted for voyeurism by the operators of one public-surveillance system. Studies of operators of public-surveillance systems have also shown instances of selectively monitoring dark-skinned persons. Further, powerful surveillance tools may offer a tempting aid to repression of groups such as political protestors. Many aspects of public-space behaviors that are quite legal are nevertheless confidential or at least personal by nature—courtship behaviors, travel patterns, buying habits, lawyer/client consultations, reading choices, smoking, and more. Many persons dislike the idea of such behaviors being recorded by government officials as a matter of course.

There is also widespread willingness in some countries, however, to give up a large measure of privacy in the quest for security from terrorism. A survey conducted by *Business Week* in November, 2001 found that 63% of U.S. adults favored increasing use of public-surveillance CCTV and that 86% favored the use of facial-recognition software to scan for terrorists in public places (as was done with taped images of over 100,000 attendees at the 2001 Superbowl). CCTV, enhanced by computer processing, will probably play a growing role in both its traditional security applications and in public life in years to come.

#### ■ FURTHER READING:

##### BOOKS:

Nieto, Marcus, Kimberly Johnston-Dodds, and Charlene Simmons. *Public and Private Applications of Video Surveillance and Biometric Technologies*. Sacramento, CA: California Research Bureau, California Public Library, 2002.

##### PERIODICALS:

Notton, John. "The Use of Technology in Policing the City of London," in proceedings from the *International Carnahan Conference on Security Technology*, Larry D. Sanson, ed., IEEE, 35–39, 1998.

Sage, Kingsley, and Steward Young. "Computer Vision for Security Applications," in proceedings from the *International Carnahan Conference on Security Technology*, Larry D. Sanson, ed., IEEE, 210–215, 1998.

Thief, Geoff. "Automatic CCTV Surveillance: Towards the VIRTUAL GUARD," in proceedings from the *International Carnahan Conference on Security Technology*, Larry D. Sanson, ed., IEEE, 42–48, 1999.

Walters, Peter. "CCTV Operator Performance and System Design," in proceedings from the *International Carnahan Conference on Security Technology*, Larry D. Sanson, ed., IEEE, 32–37, 1993.

##### ELECTRONIC:

American Civil Liberties Union (ACLU). "What's Wrong With Public Video Surveillance?" <[http://archive.aclu.org/issues/privacy/CCTV\\_Feature.html](http://archive.aclu.org/issues/privacy/CCTV_Feature.html)> (December 19, 2002).

##### SEE ALSO

*Biological and Biomimetic Systems*

*Bio-Optic Synthetic Systems (BOSS)  
Biosensor Technologies*

## Coast Guard (USCG), United States

■ CARYN E. NEUMANN

One of the world's leading maritime security forces, the United States Coast Guard (USCG), maintains public safety in American ports and shipping lanes while also enforcing laws against drug trafficking, environmental abuses, and illegal immigration. Created from a 1915 merger of the Life Saving Service and the Revenue Cutter Service, the Coast Guard is unique among the nation's armed services in that it has two masters. The Coast Guard has historically been attached to the U.S. Navy during times of war, but as of March 1, 2003, the Coast Guard acts under the direction of the Department of Homeland Security (transferred from the Department of Transportation). The USCG plays a major role in homeland security by screening passenger arrivals and conducting inspections at critical domestic ports as well as engaging in patrols of the American coastline.

The Coast Guard traces its origins to a 1790 act of Congress authorizing the construction of vessels to enforce tariff and trade laws, prevent smuggling, and protect the collection of the federal revenue. The Revenue Cutter Service that grew out of this order gradually assumed the additional duties of derelict destruction, protection of game, and enforcement of environmental laws. When the Revenue Cutter Service merged with the Life Saving Service, the newly formed USCG constituted a new branch of the military but a relatively poorly armed one. For most of its existence, the USCG has relied on light weapons that could be brought topside upon need while vessels operating inland generally had only small arms aboard. In war, USCG ships would add mounted guns, but such weaponry has not been deemed necessary for the routine peacetime activities of combating smuggling, assisting ships in distress, and conducting patrols.

The task assigned to the USCG is a daunting one. Over 95% of America's overseas trade moves by sea through 361 ports along 95,000 miles of coastline. It is more economical to bring in drugs and other illegal products in bulk by sea instead of by air, a fact that has prompted numerous traffickers to try their luck at evading the Coast Guard. To combat maritime smuggling, the service designed radar especially for marine traffic surveillance and control in 1972. At first, only operational in the key ports of San Francisco, Houston, Galveston, New Orleans, Puget Sound, and New York, radar is now commonly used, but the chief counter-smuggling activity of the Coast Guard remains the patrol of American waters by





Members of a six-man U.S. Coast Guard law enforcement Tactical Team North, operating from the USS *Typhoon*, approach the tank vessel *Kara Sea*, designated a high interest vessel because of its gasoline cargo, in the Chesapeake Bay in August 2002. AP/WIDE WORLD PHOTOS.

ships and aircraft. In strategic ports, the USCG works closely with the U.S. Navy to protect naval assets. It has developed a methodology to conduct port vulnerability assessments to identify critical infrastructure and is in the process of establishing port security units to be rapidly deployed to provide law enforcement in the event of emergencies such as terrorist attacks.

About half of the USCG's resources are dedicated to public safety, a percentage that has increased in response to the attacks of September 11, 2001. In order to guard against future terrorist assaults, the Coast Guard screens crew and passenger lists obtained through the advance notice of vessel arrival forms that must be completed by all ships. It has developed a maritime homeland security strategy that involves coordinating USCG activities with the intelligence community, U.S. Customs Service, U.S. Navy, Border Patrol, and Immigration and Naturalization Service; sharing maritime intelligence with other nations; and conducting layered maritime security operations with the aim of deterring, disrupting, and intercepting threats before such dangers can reach American shores.

The survival of the Coast Guard seems assured. Congressional assertions that many of the duties of the USCG could be carried out more cheaply by private contractors have ceased as the threat of terrorism increases. Uniquely

positioned to continue to provide the maritime component of homeland security, the USCG has decades of experience in detecting and intercepting unwanted intruders without significantly disrupting the transportation system.

#### ■ FURTHER READING:

##### BOOKS:

Gottschalk, Jack A. and Brian P. Flanagan. *Jolly Roger with an Uzi: The Rise and Threat of Modern Piracy*. Annapolis: Naval Institute Press, 2000.

Johnson, Robert Erwin. *Guardians of the Sea: History of the United States Coast Guard, 1915 to the Present*. Annapolis: Naval Institute Press, 1987.

##### PERIODICALS:

Hessman, James D. "The Maritime Dimension; Special Report: The Coast Guard's Role in Homeland Defense." *Sea Power* (Apr 2002), pp. 26–30.

##### ELECTRONIC:

United States Department of Transportation. "United States Coast Guard." January 27, 2003. <<http://www.uscg.mil/USCG.shtm.asp>> (January 27, 2003).

## SEE ALSO

*Coast Guard National Response Center*  
*Crime Prevention, Intelligence Agencies*  
*Customs Service, United States*  
*DEA (Drug Enforcement Administration)*  
*INS (United States Immigration and Naturalization Service)*  
*NMIC (National Maritime Intelligence Center)*  
*September 11 Terrorist Attacks on the United States*

## Coast Guard National Response Center

### ■ JUDSON KNIGHT

The Coast Guard National Response Center (CGNRC) is the sole national point of contact for reports of oil spills, as well as information regarding discharges of chemical, radiological, and biological discharges into the environment. As a unit of the Coast Guard, CGNRC is part of the Department of Transportation (DOT), but due to the significance of its function, it often reports directly to the president of the United States. The increased terrorist threat following the attacks of September 11, 2001, have only served to further its importance as part of the homeland security apparatus.

The federal government advises individuals who observe oil spills, or evidence of oil spills, in or around the United States, to report that information to CGNRC. The latter will dispatch on-scene coordinators to collect data, and will serve as a liaison for the U.S. National Response Team (NRT). However, the responsibilities and purview of CGNRC extend far beyond the functions one normally associates with the Coast Guard. Not only is CGNRC the principal point of contact regarding oil spills, the same is true with regard to chemical, radiological (having to do with nuclear radiation), biological, and etiological (involving disease) hazards as well.

**Working with other departments and agencies.** CGNRC assists a vast array of government departments, agencies, and administrations in myriad ways. For the Federal Emergency Management Agency, for instance, it acts as a contact point on reports of natural disasters and the evacuations associated with them. The Federal Railroad Administration (FRA) depends on its 24-hour Rail Emergency Hotline, which receives and disseminates information on hazards ranging from railroad accidents to the refusal of railroad employees to undergo drug testing. CGNRC assists the Department of Defense (DoD) by recording transportation incidents or anomalies involving DoD explosives or other sensitive materials, while the Department of the Interior relies on CGNRC to receive reports of incidents involving Trans-Alaskan Pipeline Oil.

In addition to regularly briefing the secretary of Transportation and the chiefs of modal administrations (e.g., the FRA) regarding transportation emergencies, CGNRC also conducts briefings for the White House and the Department of Homeland Security. In the aftermath of the 9–11 terrorist attacks, the federal government has urged civilians witnessing any suspicious activity around rivers and waterways to report this information to CGNRC. According to the New Orleans *Times-Picayune* in November 2002, “Activities that should be reported include unusual filming, hunting or fishing in unusual areas, lights flashing between boats and the shore, ship crew members recovering or tossing things into the water, and divers entering the water near docks or bridges.” Numbers for contacting CGNRC are provided at its Web site, listed below.

### ■ FURTHER READING:

#### PERIODICALS:

Darce, Keith. “Port Still Vulnerable, Its Chief Says.” *Times-Picayune*. (New Orleans, LA) (November 20, 2002): 1.  
 Kreuzer, Heidi. “Westchester Incident Highlights Oil Spill Concerns.” *Pollution Engineering* 33, no. 1 (January 2001): 9–10.

#### ELECTRONIC:

Coast Guard National Response Center. <<http://www.nrc.uscg.mil/index.htm>> (January 22, 2003).  
 U.S. National Response Team. <<http://www.nrt.org/production/nrt/home.nsf>> (January 22, 2003).

### SEE ALSO

*Coast Guard (USCG), United States*  
*Homeland Security, United States Department*  
*National Response Team, United States*

## Code Name

A code name is a word or phrase used to refer secretly to a specific person, group, project, or plan of action. Individual spies and large-scale military operations are often referred to by code names to protect their identity. For example, the code name for the United States’ project to produce an atomic bomb during World War II was “Manhattan Project,” the codename for the U.S. plan to invade Okinawa on April 1, 1945 was “Iceberg,” the Nazi German plan to invade England had the code name “Operation Sea Lion,” and the code name of Spanish double agent Juan Pujol Garcia, who spied for the British while pretending to spy for the Nazis, was “Garbo.” So common is the use of code names that an entire book has been devoted to cataloguing the code names used during World War II.

A code name is a particular type of code word. A code word is any word or phrase that has been chosen to signify a specific message while keeping that message hidden from a third party. Functional codes may contain thousands of code words, some of which may also be code names; however, a code name need not be part of a larger code. It may, in effect, be a code unto itself, comprised of only one word.

#### ■ FURTHER READING:

##### BOOKS:

- Chant, Christopher. *The Encyclopedia of Codenames of World War II*. London: Routledge & Kegan Paul, 1986.
- Churchouse, Robert. *Codes and Ciphers*. Cambridge, UK: Cambridge University Press. 2002.
- Mollin, Richard A. *An Introduction to Cryptography*. New York: Chapman & Hall 2001.
- Singh, Simon. *The Code Book*. New York: Doubleday, 1999.

##### SEE ALSO

*Code Word*  
*Codes and Ciphers*

## Code Word

A code word is a word or phrase that is used to convey a predefined message that differs from its own literal meaning. For example, the code word IRONBOUND might be used to convey the message “meet by the river at midnight.” If a number (e.g., 785) is used instead of a word, it is termed a code number. Both code words and code numbers are also termed code groups.

A code is comprised of a list of messages and the code groups that have been defined for them, usually written down in parallel columns in a codebook. To create or interpret messages in a code, one must have access to its codebook. One advantage of a code, as compared to a cipher, is that a single code group may contain a variable amount of information, even within a single code; the code word IRONBOUND, above, conveys a complete command, while another code word might stand either for a single word or for an entire plan of operation. This makes a well-designed code difficult to crack by examining captured messages for patterns.

Word codes, however, also have disadvantages. First and foremost, if a copy of the codebook falls into enemy hands, then the code becomes useless. Second, only ideas for which code words have been predefined can be communicated using a given code. For example, if a code book contains no code word for “noon,” it may be impossible to convey the message, “meet by the river at noon.”

Codes are therefore limited in flexibility by the number of code words that can be fit into a code book of practical size, whereas ciphers can convey almost any written message .

#### ■ FURTHER READING:

##### BOOKS:

- Mollin, Richard A. *An Introduction to Cryptography*. New York: Chapman & Hall, 2001.
- Singh, Simon. *The Code Book*. New York: Doubleday, 1999.

##### SEE ALSO

*Code Name*  
*Codes and Ciphers*

## Codes and Ciphers

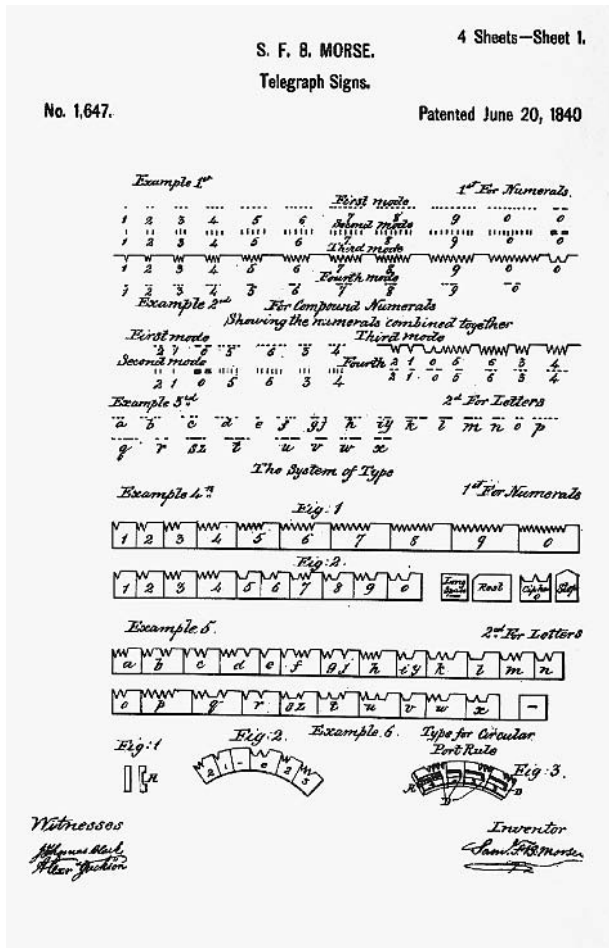
#### ■ LARRY GILMAN

Codes and ciphers are forms of cryptography, a term from the Greek *kryptos*, hidden, and *graphia*, writing. Both transform legible messages into series of symbols that are intelligible only to specific recipients. Codes do so by substituting arbitrary symbols for meanings listed in a codebook; ciphers do so by performing rule-directed operations directly on original message text. Because codes can only communicate concepts that are listed in their codebooks, they have limited flexibility. Rather, modern cryptography relies almost entirely on ciphers implemented by digital computers, and is widely employed in industry, diplomacy, espionage, warfare, and personal communications.

**Codes.** A *code* is a set of symbolic strings (“code groups”) that are listed, along with their assigned meanings, in a code book.

Codes encrypt messages by substitution, that is, they substitute code groups for components of the original message. “Kill the king at midnight” could thus be encoded, for example, as “OAKEN 7890 SPINDRIFT.” Without the code book, it would be difficult for a reader of the encoded message to form an idea of its meaning.

Either a word or a number can be used as a code group. Code groups that are words are termed code words and those that are numbers are termed code numbers. Note that a single code group can encode a single word (“king”) or an entire phrase (“deliver the films to agent number 3”). A coded message may, therefore, be shorter than the original message. It can also be made as long as or longer than the original message, if the codebook



The Morse Code, named for inventor Samuel Morse, was patented in this form in 1840. This code is regarded as one of the great steps forward in international communication. ©BETTMANN/CORBIS.

provides lengthy code phrases for single concepts or nonsense code groups for padding purposes. Such techniques can be used to make encoded messages harder for opponents to read.

**Ciphers.** A cipher uses a system of fixed rules (an "algorithm") to transform a legible message ("plaintext") into an apparently random string of characters ("ciphertext"). For example, a cipher might be defined by the following rule: "For every letter of plaintext, substitute a two-digit number specifying the plaintext letter's position in the alphabet plus a constant between 1 and 73 that shall be agreed upon in advance." If 46 is the agreed-upon constant, then the plaintext word ZAP enciphers to 724762 as follows:

- Plaintext letter Z = ciphertext 72 (alphabet position 26 + 46).
- Plaintext letter A = ciphertext 47 (alphabet position 1 + 46).

- Plaintext letter P = ciphertext 62 (alphabet position 16 + 46).

Incorporation of a variable term into a fixed algorithm, as in this example, is typical of real-world ciphers. The variable component is termed a key. A real key would be longer and would have a more complex relationship to the cipher algorithm than the key in this example, but its basic role would be the same: a key fits into an algorithm so as to enable enciphering and deciphering, just as a physical key fits into a lock to enable locking and unlocking. Without a key, a cipher algorithm is missing an essential part. In fact, so important is the concept of the key that in real-world ciphering it is not algorithms that are kept secret, but keys. Cipher designers assume that their algorithms will always become known to their opponents, but design the relationship between key and algorithm so that even knowing the algorithm it is almost impossible to decipher a ciphertext without knowing the appropriate key. Before a cipher can work, therefore, a key or set of keys must be in the possession of both the sender and the receiver.

If the key were always the same, it would simply constitute a permanent part of the algorithm, and keying would have no special advantage over trying to keep one's algorithm secret to begin with. Keys must, therefore, be changed occasionally. A new key may be employed every day, for every message, or on some other schedule.

**Comparison of codes and ciphers.** Codes have the advantage of simplicity. No calculations are required to encode or decode messages, only lookups in a codebook. Further, because a code uses no fixed system for associating code groups with their meanings (even the amount of meaning assigned to a code word can vary, as seen above), a code may fail gracefully—that is, an enemy may discern the meaning of a few code groups but still be unable to interpret others. In contrast, a cipher produces ciphertext from plaintext (and vice versa) according to a fixed algorithm. Thus, if an enemy determines the algorithm and steals or guesses a key, they can at once interpret all messages sent using that key. Changing the key may restore cipher security, unless the enemy has developed a system for guessing keys. One such system, always possible in theory, is to try all possible keys until one is found that works.

Codes, however, have two great disadvantages. Users can only send messages that can be expressed using the terms defined in the codebook, whereas ciphers can transmit all possible messages. Additionally, all codes are vulnerable to codebook capture. If a codebook is captured, there is no recourse but to distribute new codebooks to all users. In contrast, the key–algorithm concept makes cipher secrecy dependent on small units of information (keys) that can be easily altered.

Secure ciphers, however, entail complex calculations. This made the use of complex ciphers impractical before



A 1968 miniature Kroger's codebook containing a series of numbers that was used by spies to decode messages from Moscow, displayed beside an enlarged photocopy of the text. ©HULTON-DEUTSCH COLLECTION/CORBIS.

the invention of ciphering machines in the early twentieth century; codes and simple ciphers were the only feasible methods of ciphering. Yet, a cipher that is simple to implement is proportionately simple to crack, and a cracked cipher can be disastrous. It is better to have to communicate "in the clear"—to send messages that can be easily read by the enemy—than to suppose that one's communications are secret when they are not. Mary, Queen of Scots (1542–1567) was executed for treason on the basis of deciphered letters that frankly discussed plans for murdering Queen Elizabeth of England; likewise, simple ciphers used by the Confederacy during the U.S. Civil War were easily cracked by Union cryptographers. What is more, even more sophisticated ciphers, such as the Enigma cipher used by Nazi Germany during World War II or implemented today on digital computers, are subject to attack. As soon as any new cipher is invented, someone, somewhere starts attacking it. The result is that ciphers, like some antibiotics, have limited lifespans, and must be regularly replaced.

**Historical perspective.** Throughout much of the ancient world, writing was either completely unknown or was an

arcane art accessible only to priests. There was little motive, therefore, to develop coding or ciphering. Eventually, however, writing came to serve military, personal, and commercial as well as sacred purposes, creating a need for secure communications. To meet this need, ciphers based on scrambling the order of plaintext characters or on substituting other characters for them were developed. The first recorded use of ciphering was by the Greek general Lysander in the fifth century B.C. The *Kamasutra*, a Hindu text compiled in the A.D. fourth century from manuscripts dating back as far as the fourth century B.C., recommends monoalphabetic substitution ciphering—the replacement of each letter of a plaintext message with a different letter of the alphabet—as one of the 64 arts to be mastered by an ideally-educated woman. By the first century B.C., codes had also been developed.

Cryptography fell out of use during the early Middle Ages, but Arab scholars during the heyday of medieval Muslim civilization, the Abbasid caliphate (A.D. 750–1258), revived it. Muslim writers not only ciphered, but invented *cryptanalysis*, the systematic breaking of ciphers. Ninth-century Arab philosopher Abu Yusuf al-Kindi wrote the earliest known description of the cryptanalytic technique known as frequency analysis, which breaks substitution

ciphers by matching ciphertext letters with plaintext letters according to their frequency of use in the language. In English, for example, the most frequently used letter is E; in an English-language ciphertext produced using a monoalphabetic substitution cipher, therefore, the most frequently used character probably stands for E.

During the late Middle Ages and the Renaissance, a literate ruling class arose throughout Europe, and ciphering regained importance in that part of the world for purposes of intrigue, espionage, and war. English monk and scientist Roger Bacon (1220–1292) wrote a book describing several cryptographic methods; Italian artist Leon Battista Alberti (1404–1472) wrote the first European text on cryptanalysis in 1466. Under pressure from cryptanalysis, codes and cipher systems gradually became more complex.

Beginning in the mid-nineteenth century, the importance of coding and ciphering was rapidly amplified by the invention of electronic information technologies: the telegraph (1837), the telephone (1876), radio (1895), and electronic computers (1940s). Non-secret commercial codes were developed in conjunction with telegraphy to make messages more compact (therefore cheaper); ciphers were widely used (and cracked) during the U.S. Civil War and the first and second world wars. The cracking of German and Japanese ciphers by Allied cryptographers during World War II was of particular importance, enabling the British and Americans to avoid submarines, intercept ships and aircraft, and otherwise frustrate enemy plans. Ciphering has since become basic to military and government communications. Since the 1960s, commercial and personal communications have become increasingly dependent on digital computers, making sophisticated ciphering a practical option for those sectors as well. In the late 1970s, the U.S. government defined a cipher algorithm for standard use by all government departments, available also to the public; this now-elderly algorithm, the Digital Encryption Standard, is today in the process of being replaced by a new algorithm, the Advanced Encryption Standard.

**Types of codes.** Codes can be generally divided into *one-part* and *two-part* codes. In a one-part code, the same codebook is used for encipherment and decipherment. The problem with this system is that some systematic ordering of the code groups and their assigned meanings must be made, or it will be difficult to locate code groups when enciphering or their meanings when deciphering. (A randomly ordered list of words or numbers thousands of terms long is difficult to search except by computer.) Thus, code groups tend to be arranged in alphabetic or numerical order in a one-part code, an undesirable property, since an opponent seeking to crack the code can exploit the fact that code groups that are numerically or alphabetically close probably encode words or phrases that are alphabetically close. To avoid this weakness, a two-part code employs one codebook for encipherment and another for decipherment. In the encipherment codebook,

alphabetically ordered meanings (e.g., A, ABDICATE, ABLE) are assigned randomly ordered code groups (e.g., 6897, 1304, 0045). In the decipherment codebook, the code groups are arranged in order (e.g., 0045, 1304, 6897), for easy location.

Code security can be improved by combining ciphering with coding. In this technique, messages are first encoded and then enciphered; at the receiving end, they are first deciphered and then decoded. A standard method for combining coding and ciphering is the “code plus additive” technique, which employs numbers as code groups and adds a pseudorandom number to each code group to produce a disguised code group. The pseudorandom numbers used for this purpose are generated by modular arithmetic techniques closely related to those used in stream ciphering.

**Block ciphers.** Ciphers that encrypt whole blocks of characters at once—such as 10 letters at a time, or 128 bits—are termed block ciphers. Block ciphers have the advantage that each character in each ciphertext block can be made to depend complexly on all characters of the corresponding message block, thus scrambling or smearing out the message content over many characters of ciphertext. The widely used Digital Encryption Standard (DES) is a block cipher that employs a 56-bit key to encrypt 56-bit blocks. In DES, the key and each message block are used as inputs to a complex algorithm that produces a 56-bit block of ciphertext. The same key is used to decode the block of ciphertext at the receiving end.

**Stream ciphers.** Stream ciphers operate upon series of binary digits (“bits,” usually symbolized as 1s and 0s), enciphering them one by one rather than in blocks of fixed length. In stream encipherment, a series of bits termed the key-stream is made available by some means to both the sender and receiver. This stream is as long as the message to be sent. At the sending end, the key-stream is combined with the message-stream in a bit-by-bit fashion using the exclusive or operation of Boolean algebra, producing the ciphertext. At the receiving end, the same key-stream is combined again with the ciphertext to recover the message stream. This system of ciphering is unbreakable in both theory and practice if the key-stream remains secret. Ongoing breakthroughs in quantum cryptography may soon make perfectly secret key-streams available by exploiting certain properties of photons. If these techniques can be made technologically practical, truly unbreakable cipher systems will have become available for the first time in history.

**Public-key ciphers.** All ciphers require the use of a secret key. Public-key ciphers, first developed in the late 1970s, are no exception. However, public-key ciphers have the

important advantage that the secret key possessed by the sender need not be the same secret key possessed by the receiver; thus, no secure transfer of keys between the sender and receiver is ever necessary.

Public-key ciphers exploit the computational difficulty of discovering the prime factors of large numbers. (The prime factors of a number are the primes that, when multiplied together, produce the number: e.g., the prime factors of 15 are 5 and 3.) To create a public key, two large (50-digit or longer) primes are chosen and their product calculated. This number ( $r$ ) is made public. Further mathematical operations by the user produce two numbers based on  $r$ ; one of these is the user's public key  $k_p$ , and the other is retained as the user's private key  $k_s$ . Anyone that knows  $r$  and a given user's public key  $k_p$  can send encrypted messages to that particular user; the recipient decrypts the message using their private key  $k_s$ .

Public-key cryptography has seen wide use since the 1970s. Its security is limited by the ability of opponents to determine the prime factors of  $r$ , and the difficulty of this task is a function both of the size of  $r$  and of the speed of available digital computers. (Large  $r$  also makes encryption and decryption more computation-intensive, so it is not practical to defeat opponents by simply making  $r$  extremely large.)

Software for a powerful public-key cipher algorithm known as Pretty Good Privacy (PGP) is downloadable for free from many sites on the Internet.

**Attacking codes and ciphers.** Codes and ciphers can be attacked by two basic means. The first is theft of codebooks or keys—espionage. The second is cryptanalysis, which is any attempt to crack a code or cipher without direct access to keys or codebooks. Cryptanalysis may proceed either by trial and error or by systematic analysis of plaintext and ciphertext. The analytic approach may involve both looking for patterns in ciphertext and solving mathematical equations representing the encryption algorithm.

Cryptanalysis by trial and error usually means guessing cipher keys. A cipher key can be guessed by trying all possible keys using a computer. However, designers of encryption systems are aware of this threat, and are constantly employing larger and larger keys to keep ahead of growing computer speed. Systematic cryptanalysis may seek patterns in ciphertext, either by itself or in conjunction with a known plaintext (the so-called "known-plaintext attack"). Mathematical modeling of cipher algorithms may assist trial-and-error methods by reducing the number of guesses required to within (or near) practical limits. For example, in 2002, cryptographers announced that the recently-standardized Advanced Encryption Standard of the U.S. government might be vulnerable to a mathematical attack that would reduce the number of computations needed for a successful trial-and-error attack from order  $2^{256}$  to order  $2^{100}$ . The latter number is still not computationally practical, but may be soon.

Quantum cryptography holds out the promise of truly attack-proof ciphering. In a quantum-cryptographic system, not only would messages be undecipherable if intercepted, but also the act of interception would always be detectable by the intended receiver. Such systems may become available to military and government users around 2010.

#### ■ FURTHER READING:

##### BOOKS:

- Charthouse, Robert. *Codes and Ciphers*. Cambridge, UK: Cambridge University Press, 2002.
- Meyer, Carl H., and Stephen M. Matyas. *Cryptography: A New Dimension in Computer Data Security*. New York: John Wiley & Sons, 1982.
- Mollin, Richard A. *An Introduction to Cryptography*. New York: Chapman & Hall, 2001.
- Singh, Simon. *The Code Book*. New York: Doubleday, 1999.
- Stinson, Douglas R. *Cryptography: Theory and Practice*. New York: Chapman & Hall, 2002.

##### PERIODICALS:

- Seife, Charles. "Crucial Cipher Flawed, Cryptographers Claim." *Science* no. 5590 (2002): 2193.

##### SEE ALSO

- ADFGX Cipher*  
*Cipher Disk*  
*Cipher Key*  
*Cipher Machines*  
*Code Name*  
*ENIGMA*  
*FISH (German Geheimschreiber Cipher Machine)*  
*French Underground During World War II, Communication and Codes*  
*Playfair Cipher*  
*World War I: Loss of the German Codebook*  
*World War II, United States Breaking of Japanese Naval Codes*

---

## Codes, Fast and Scalable Scientific Computation

---

A code is a system for concealing a message by replacing words or phrases with symbols. Codes are used on computers for a number of purposes relevant to espionage and security, among them the development of large-scale scientific simulations. For this to be possible, it is necessary to develop algorithms, or mathematical processes,

that are easily scalable, or adjustable, such that computation time does not increase exponentially.

There are numerous situations for which a computer simulation is preferable to a real-life demonstration, an extreme example being a study of radiation diffusion following a nuclear blast. Performing such a study requires a computer simulation, or a program that emulates and measures the effects of a real-life process. These problems are so complex that they require parallel processing, or the use of two or more computers working in tandem, as well as the development of scalable algorithms.

An algorithm is a method for solving a mathematical problem by using a finite number of computations, usually involving repetition of certain operations or steps. A scalable algorithm is one that is capable of implementing additional computational resources in such a way as to solve increasingly more complex problems. To be truly scalable, the work required to solve an algorithm should grow at a rate smaller than the rate at which the amount of input grows.

#### ■ FURTHER READING:

##### ELECTRONIC:

Fast and Scalable Scientific Computation. Defense Advanced Research Projects Authority. <[http://www.arpa.mil/dso/thrust/am/faca\\_1.htm](http://www.arpa.mil/dso/thrust/am/faca_1.htm)> (January 27, 2003).

Scalable Linear Solvers. Lawrence Livermore National Laboratory. <[http://www.llnl.gov/CASC/sc2001\\_fliers/SLS/SLS01.html](http://www.llnl.gov/CASC/sc2001_fliers/SLS/SLS01.html)> (January 27, 2003).

##### SEE ALSO

*Computer Modeling*  
*Lawrence Livermore National Laboratory (LLNL)*  
*Supercomputers*

## COINTELPRO

#### ■ LARRY GILMAN

COINTELPRO (for Counter Intelligence Program) was a set of programs commenced by the United States Federal Bureau of Investigation (FBI) in 1956 and officially terminated in 1971. COINTELPRO included programs variously named Espionage COINTELPRO; New Left COINTELPRO; Disruption of White Hate Groups (targeting the Ku Klux Klan); Communist Party, USA COINTELPRO; Black Extremists COINTELPRO; and the Socialist Workers' Party Disruption Program. Although these were "counterintelligence" programs by name, the FBI did not consider most of these groups to be engaged in intelligence activities (e.g., spying for the Soviet Union). Rather, it deemed their political

activities dangerous, and assumed that various court decisions had made it impossible to control them by nonsecret, legal means (e.g., arrests for illegal acts). COINTELPRO began by targeting the Communist Party, but quickly expanded to include other groups. The FBI's "black extremist" category included not only the Black Panthers but the Southern Christian Leadership Conference and its president, Martin Luther King, Jr., the Student Nonviolent Coordinating Committee, and other civil rights groups of the 1950s and 1960s. COINTELPRO also targeted groups opposed to the Vietnam War.

COINTELPRO remained secret until a large number of documents were stolen from the FBI office in the town of Media, Pennsylvania, in 1971. Lawsuits brought by political groups who believed that they were being observed and disrupted by the FBI soon produced other COINTELPRO-related documents. In 1975, a Senate committee—the Select Committee to Study Governmental Relations with Respect to Intelligence Activities, better known as the Church Committee after its chair, Senator Frank Church (D, Idaho)—was appointed to investigate COINTELPRO and other domestic espionage and disruption programs conducted by the FBI, the Central Intelligence Agency, the National Security Agency, Army intelligence, and the Internal Revenue Service. The Church Committee concluded in 1976 that "the domestic activities of the intelligence community at times violated specific statutory prohibitions and infringed the constitutional rights of American citizens," and stated that the FBI had gathered information by illegal means, disseminated that information illegally, and otherwise violated the law in its efforts to disrupt political activities that it considered subversive. The committee's report stated that "the abusive techniques used by the FBI in COINTELPRO from 1956 to 1971 included violations of both federal and state statutes prohibiting mail fraud, wire fraud, incitement to violence, sending obscene material through the mail, and extortion. More fundamentally, the harassment of innocent citizens engaged in lawful forms of political expression did serious injury to the First Amendment guarantee of freedom of speech and the right of the people to assemble peaceably and to petition the government for a redress of grievances."

Disruption techniques used by the FBI during COINTELPRO, according to the findings of the Church Committee, included burglaries; illegal opening and photographing of first-class mail; planting of forged documents to make it appear that individuals were government informants; anonymous letters to spouses, designed to break up marriages; secretly communicating with employers in order to get individuals fired; planting of news articles and editorials (covertly authored by FBI agents) in U.S. magazines and newspapers; anonymous letters containing false statements designed to encourage violence between street gangs and the Black Panthers; anonymous letters denouncing Catholic priests who allowed their churches to be used for Black Panther breakfasts sent to their bishops; requests for selective tax audits; encouragement of violent tactics by paid FBI informants posing as



members of antiwar groups in order to discredit those groups; and others.

■ FURTHER READING:

ELECTRONIC:

"Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities." United States Senate. April 26, 1976. <<http://www.derechos.net/paulwolf/cointelpro>> (March 18, 2003).

---

## Cold War (1945–1950), The Start of the Atomic Age

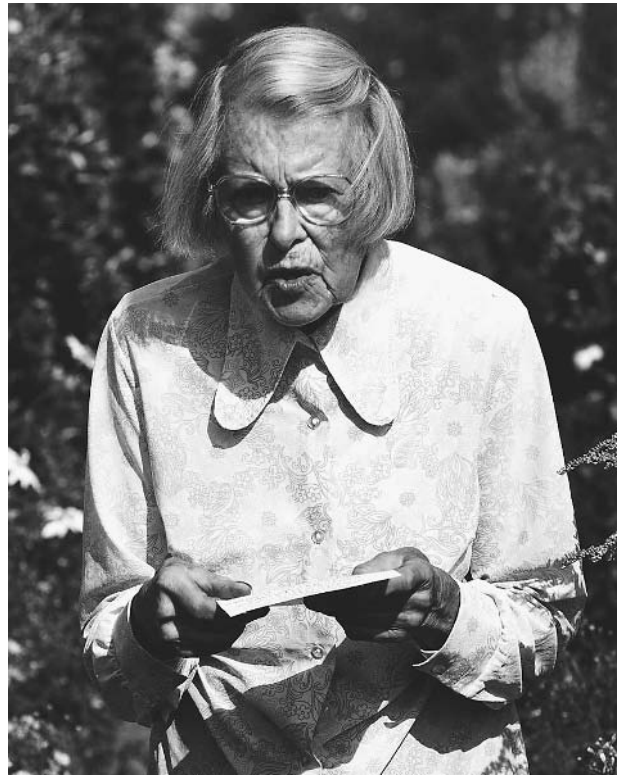
---

■ SIMON WENDT

The Cold War was an ideological, political, economic, and military conflict between the United States and the Union of Soviet Socialist Republics (U.S.S.R.), which began in the aftermath of World War II and ended in 1989. From the outset, the Cold War was inextricably linked with the development of the atomic bomb and its use as a military deterrent.

**Roots of the Cold War.** The enmity between the United States and Russia, the largest of the fifteen republics that ultimately constituted the U.S.S.R., stemmed from a long history of mutual distrust. Opposing plans concerning the political and economic future of post-World War II Europe and disputes concerning the development and control of atomic weapons intensified the conflict. The seeds of antagonism date back to 1917. That year, the United States dispatched a contingent of soldiers to assist European allies in overthrowing Russia's new communist regime, which had come to power during the Russian Revolution. Despite the operation's failure, the U.S. government continued to deny the new Soviet Union diplomatic recognition until 1933. After a brief period of cooperation, Russian leaders' suspicions toward America began anew at the dawn of World War II. They considered Western nations' initial refusal to oppose Nazi Germany and Japan with arms part of a capitalist scheme to destroy the U.S.S.R. Americans, on the other hand, assumed that the brutal regime of Soviet dictator Joseph Stalin (1879–1953) was only slightly better than that of Germany's leader Adolph Hitler (1889–1945).

During World War II, Stalin's doubts about the sincerity of American vows to support the Soviet war effort intensified. Soon after the beginning of the war in 1939,



Melita Norwood, an 87-year-old great-grandmother, reads a statement outside her London home after being unmasked as one of the Soviet Union's top Cold War spies who passed atomic secrets to Moscow, giving the Soviet Union a vital edge in the arms race. ©REUTERS NEWMEDIA INC./CORBIS.

the Soviet Union bore the brunt of military action, attempting to fend off a massive German invasion. Although American President Franklin D. Roosevelt (1882–1945) promised the Soviet leader substantial economic aid, the United States managed to provide relatively few supplies. More important, Roosevelt assured Stalin in 1942 that American troops would relieve some of the military pressure on Russia by establishing a second front in Western Europe. However, logistical and production problems postponed an allied invasion for several years. When allied forces finally landed on Europe's shores on June 6, 1944, Roosevelt had reneged on his promise three times. This delay burdened post-World War II U.S.-Soviet relations considerably.

Even before Germany's surrender on May 9, 1945, additional disputes arose over the future of liberated Europe. The United States envisioned democratic and freely elected societies based on the right of self-determination and free trade. By contrast, the Soviet Union sought territorial expansion and spheres of influence that would guarantee the country's national security. Accordingly, during and after the war, Stalin insisted on establishing Eastern European governments supportive of the Soviet Union. He considered countries such as Poland, Bulgaria, and Romania part of an essential buffer zone to prevent future

attacks on the territory of the U.S.S.R. However, this demand was the exact opposite of President Roosevelt's vision of self-determination. These disagreements were aggravated by the U.S. government's decision to provide economic aid with the stipulation that Stalin revoke his adamant stance on the territorial question.

**Beginning of the Atomic Age.** The atomic bomb became the final divisive issue, contributing to the ultimate breakdown of U.S.-Soviet relations. In late 1938, German physicists had discovered that uranium atoms undergo fission when bombarded by neutrons. They found that this fission triggered a self-sustaining atomic reaction that could release enormous amounts of energy. Their discovery had significant potential for the development of a powerful new weapon. In 1939, a group of European émigré scientists in the United States verified the possibility of a nuclear chain reaction. The group's leader, Hungarian physicist Leo Szilard (1898–1964), worried that Nazi Germany might use this knowledge to develop an atomic bomb. In August 1939, Szilard asked famous physicist Albert Einstein (1879–1955) to sign a warning letter to President Roosevelt to convince him of the necessity to forestall German scientists. But only in early 1942 did the U.S. government finally launch an official research project to develop the new weapon.

In what the United States Army code-named Manhattan Engineer District (later dubbed Manhattan Project) scientific director J. Robert Oppenheimer (1904–1967) assembled a team of American and British scientists and engineers who developed two weapon designs. One relied on the rare Uranium-235. The other, more complicated, design used man-made Plutonium-239, which was produced in nuclear reactors that University of Chicago physicist Enrico Fermi (1901–1954) had invented in 1942. By 1944, three large reactors produced uranium and plutonium for the first American bombs. On July 16, 1945, Manhattan Project scientists tested the Plutonium weapon near Alamogordo, New Mexico, setting off the world's first nuclear explosion.

The decision by President Roosevelt's successor Harry S. Truman (1884–1972) to use atomic bombs in the military conflict with Japan proved the destructive power of nuclear weapons to the world. On August 6, 1945, a B-29 aircraft dropped a Uranium bomb over Hiroshima, Japan, obliterating the city and instantly killing 100,000 civilians. Three days later, a Plutonium bomb killed another 30,000 Japanese citizens at Nagasaki. On August 14, 1945, Japan finally surrendered. Thus, the last chapter of World War II marked the beginning of the atomic age.

The nuclear attack on Japan and the secrecy that surrounded the development of the bomb increased the tensions between the United States and the U.S.S.R. Neither President Roosevelt nor Truman was willing to share information on the bomb with the Soviets. American scientists' appeals to inform Stalin of the new research

were ignored. Rather, President Truman sought to use his country's atomic monopoly as leverage in the worsening conflict. Soviet scientists had already learned of the Manhattan Project during World War II through espionage, however, and were now coordinating their own research project on nuclear weapons. They used detailed plans that Soviet spies had supplied them. German-born physicist Klaus Fuchs (1911–1988) in particular provided crucial intelligence that facilitated the acquisition of the atomic bomb by the Soviet Union. As early as 1941, when working on Great Britain's nuclear program, Fuchs began to relay classified information to Russia. Later working on the Manhattan Project, he provided Soviet scientists with facts on virtually every aspect of the project's research. When the U.S.S.R. finally tested its own atom bomb on August 29, 1949, Stalin's scientists detonated a near-perfect replica of the American Plutonium weapon.

During the period between the first nuclear explosion in New Mexico and the end of America's atomic monopoly, a series of divisive events and decisions gradually established the fronts of the Cold War. The year 1946 saw increasingly belligerent language on both sides. Joseph Stalin proclaimed in early February that a new war was inevitable as long as capitalism existed. That same month, Moscow-based foreign-service officer George Kennan suggested in a secret telegram to Washington that the Soviet Union sought to expand its influence and planned to defeat its Western rivals. He argued that only long-term attentive containment of these expansive tendencies would avert disaster. Echoing Kennan's concerns in March, British Prime Minister Winston Churchill (1874–1965) warned of an "iron curtain," with which the U.S.S.R. would shackle Eastern Europe. Churchill also argued that the West needed to resist Communist expansion. Later that year, the Soviet Union provoked a major crisis when it continued to occupy Iran despite an agreement with Great Britain to leave the country after six months of post-war occupation. Threatened with military confrontation, Soviet troops eventually withdrew, but the Iran crisis further strained U.S.-Soviet relations.

The debate on the international control of atomic energy clearly reflected the increasing animosity between the two nations. The final U.S. plan that the administration's representative Bernard Baruch (1870–1965) presented to the United Nations on June 14, 1946, proposed to create an international agency that would supervise the mining of uranium and the manufacture of plutonium. Baruch's scheme encouraged nations to conduct research on the atom's peaceful use, but insisted on the American atomic monopoly. The Soviet Union rejected the plan. When U.S. scientists conducted a new series of nuclear weapon tests at the Bikini Atoll in the South Pacific in the summer of 1946, Stalin denounced it as proof of America's insincerity about international control.

In 1947, President Truman demonstrated that the Cold War already dominated American foreign policy. Early that year, concerns increased that Greece and Turkey might soon come under communist domination. In

what came to be known as the Truman Doctrine, the American president asked Congress on March 12, 1947, to authorize economic and military aid for the two nations to prevent a communist take-over. According to Truman, this was a litmus test of the willingness of the United States to stop the spread of communism everywhere in the world. Couching the conflict in ideological and moral terms, Truman proclaimed that people would have to choose between the alternatives of communist tyranny and democratic freedom. After Truman's impassioned speech, the requested aid package passed Congress easily. The Truman Doctrine prompted most Americans to view the conflict with the U.S.S.R. as a primarily ideological struggle between binary opposites of good and evil.

United States national security policy during the Truman administration revolved, however, around more than ideology. In the eyes of Washington's policy makers, American predominance depended on power, which they defined as the control of resources, industrial infrastructure, and strategic superiority. The National Security Council (NSC) and the Central Intelligence Agency (CIA), created by the National Security Act of 1947, used the same criteria when assessing potential Communist threats and American vital interests. The NSC served as a crucial strategic planning body for security policy. The CIA continued the espionage work of the wartime Office of Strategic Services (OSS). In 1950, a planning document drafted by the NSC, NSC-68, predicted an indefinite period of conflict with the Soviet Union, calling for a vast American military buildup. In the ensuing years, NSC-68 became the basis for American Cold War strategy.

Ideological premises and geostrategic security concerns were inextricably linked with American economic interests. Becoming one of the most important initiatives of the early Cold War, the Marshall Plan of 1947 served these economic interests and finalized the division of the world into two hostile camps. Drawn up by secretary of state George Marshall (1880–1959), the plan launched a massive economic aid package for the reconstruction of Western Europe. Healthy capitalist economies, Marshall argued, would provide American companies with new markets and could help weld European nations into an effective bulwark against Communism.

Although the United States invited the Soviet Union and Eastern European countries to apply for economic aid as well, negotiations soon demonstrated that Stalin would never accept the American plan. In fact, the Marshall Plan would not only allow the United States to control the distribution of aid, but would also give them access to the Soviet Union's economic records. Predictably, Stalin withdrew from the negotiations and countered the American economic aid project with the Molotov Plan, a series of bilateral trade agreements with Eastern European countries. The Soviet plan transformed these countries into a Communist counter alliance against the West.

In another confrontation, Stalin attempted to force the United States, Great Britain, and France to revoke their

decision to unify their three occupation zones in Germany. On July 23, 1948, the Soviet dictator initiated a year-long blockade of all supplies to the city of Berlin in the Russian zone. The United States responded with a well-organized air lift, which supplied the encircled city for almost one year. In the end, the air lift forced Stalin to give up the blockade. By that time, however, the Soviet Union already dominated Eastern Europe. In February, 1948, Czech and Slovak communists had toppled Czechoslovakia's democratic government and established a pro-Soviet Communist regime, adding the country to the Soviet bloc. In Hungary, Stalin also had imposed Communist rule. When the western part of Germany constituted itself as the Federal Republic of Germany in spring of 1949, the U.S.S.R. initiated the permanent division of the country by establishing the German Democratic Republic in the former Russian occupation zone. On April 4, 1949, the United States, Canada, and ten Western European nations had reacted to Soviet hostilities forming the North Atlantic Treaty Organization (NATO), a military alliance designed to protect its members against a potential Soviet attack.

Thus, by 1950, the framework of the Cold War was firmly in place, prompting both sides to enhance their military capabilities, in particular their nuclear arsenal. By the beginning of the new decade, the United States had amassed three hundred nuclear weapons. However, since the American administration had learned in early September, 1949, that the Soviet Union had successfully tested an atomic bomb, American policy makers considered that the strategic superiority of the United States might be in jeopardy. As a result, President Truman ordered American scientists to develop a weapon that was even more powerful: the hydrogen bomb. By the mid-1950s, both nations had developed and tested this new weapon, marking the beginning of a new round of Cold War confrontations.

#### ■ FURTHER READING:

##### BOOKS:

- Carlisle, Rodney P., with Joan M. Zenzen. *Supplying the Nuclear Arsenal: American Production Reactors, 1942–1992*. Baltimore: John Hopkins University Press, 1996.
- Gaddis, John L. *The United States and the Origins of the Cold War*. rev. ed. New York: Columbia University Press, 2000.
- . *We Now Know: Rethinking Cold War History*. New York: Oxford University Press, 1997.
- Herken, Gregg. *Cardinal Choices: Presidential Science Advising from the Atom Bomb to SDI*. rev. and exp. ed. Stanford, CA: Stanford University Press 2000.
- Holloway, David. *Stalin and the Bomb: The Soviet Union and Atomic Energy, 1939–1954*. New Haven, CT.: Yale University Press, 1994.
- Leffler, Melvyn P. *A Preponderance of Power: National Security, the Truman Administration, and the Cold War*. Stanford, CA: Stanford University Press, 1992.

Roleff, Tamara. ed. *The Atom Bomb*. San Diego, CA: Greenhaven Press, 2000.

#### SEE ALSO

*Berlin Airlift*  
*CIA (United States Central Intelligence Agency)*  
*National Security Act (1947)*  
*NATO (North Atlantic Treaty Organization)*  
*NSC (National Security Council)*  
*Nuclear Reactors*  
*OSS (United States Office of Strategic Services)*  
*Truman Administration (1945–1953), United States National Security Policy*  
*United States, Intelligence and Security*

## Cold War (1950–1972)

■ CHRISTOPHER T. FISHER

The Cold War, a contest between antithetical ideologies, democratic capitalism and Soviet socialism, emerged shortly after World War II and dominated global politics for the latter half of the twentieth century. Its origins, however, go back to the late nineteenth century when the United States decried Russia's colonial claims on the Manchurian region of China. In the early twentieth century, opposition stiffened further over Russia's brutal pogroms against its Jewish citizens. The Bolshevik cooptation of the peasant revolution against the Russian Czar in 1917, and their subsequent creation of the Soviet state, heightened mutual suspicion and opened the gulf between Russia and the West. World War II brought a temporary reprieve in animosities, but tensions reemerged over questions concerning the postwar world. President Harry Truman, successor to Franklin Delano Roosevelt, launched the first blow in the Cold War by insisting that Russia honor its prewar commitment to self-determination under the Atlantic Charter, and permit a democratic government in Poland. Soviet leader Joseph Stalin steadfastly refused any concession, and the Polish issue became the first beachhead in Cold War politics. The Polish crisis alarmed American leaders who interpreted it as confirmation that Russia intended to carry the Bolshevik revolution westward.

The thaw caused great anxiety in the United States as it turned to the Pacific theater and planned the settlement of Germany. Each situation loomed ominously with the prospect of an entrenched Soviet presence clouding negotiations. These fears compelled Truman to end the Japanese campaign as swiftly as possible. The administration made the decision to deploy the world's first atomic bomb with both the unyielding Japanese and intransigent Russians in mind.

Once the Japanese surrendered in the summer of 1945, the Cold War began in earnest. In almost rapid succession, the threat of Communist infiltration troubled

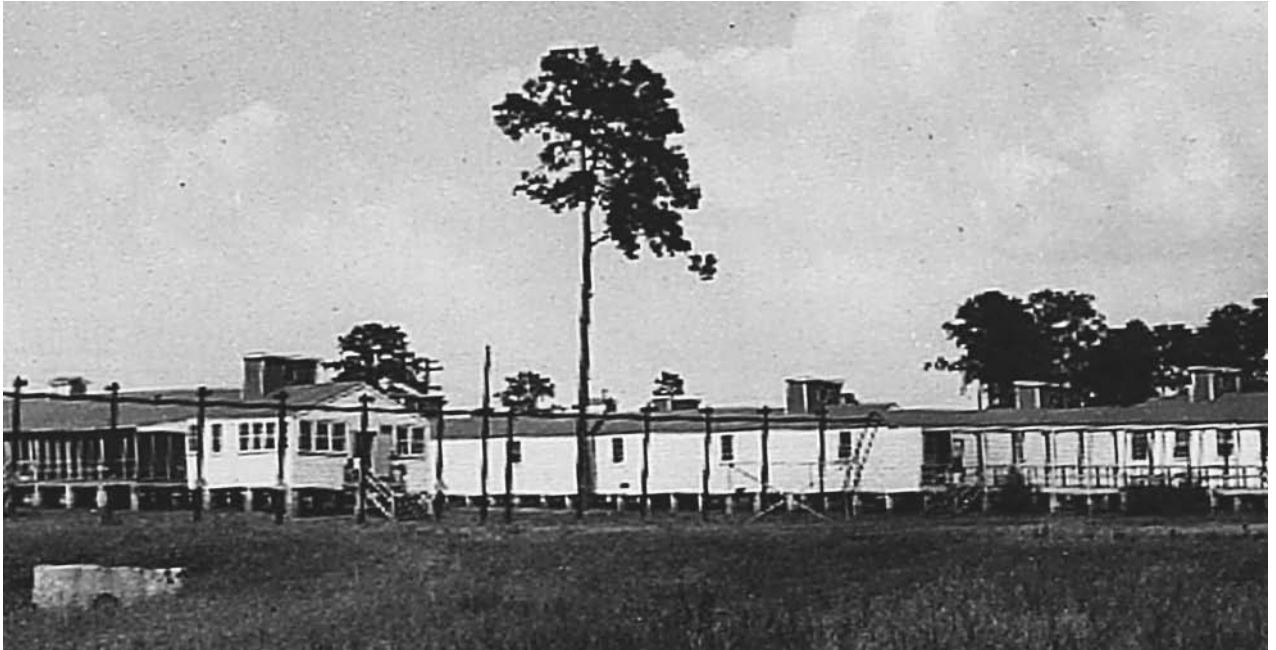
Truman. The war left many nations, particularly those in the Third World, vulnerable to Communist influence. Additionally, a few countries, most notably China, erupted in civil war between Capitalist and Communist factions at the close of World War II. The loss of China's vast natural resources, unlimited commercial potential, and immense population concerned American policymakers, who had supported the ultra-nationalist Chiang Kai Shek from the conflict's inception. To Truman's dismay, Communist leader Mao Tse Tung's made significant strides in battles as early as 1946 and gained the upper hand permanently, forcing Chiang off the mainland to the neighboring island of Taiwan, in 1949.

Simultaneous to the Chinese civil war were political fluctuations in the Middle East. The Soviet schemes on making Iran, Turkey, and Greece strategic footholds in the Mediterranean compelled Truman to take a tough stance. In 1946, America funneled well over \$600 million in appropriations to democratic forces battling the Communist led and funded National Liberation Front in Greece for control in the upcoming national elections. While in Iran and Turkey, Truman met Soviet incursions through the newly formed United Nations and with the threat of American military reprisal.

George F. Kennan, charge d'affaires in Russia, provided a rationalization for the events of 1946 in his alarm driven 8000 word dispatch from Moscow on the Soviet postwar intentions. Providing the first part in what became the intellectual mooring of the Cold War, his long telegram depicted Russia as irretrievably expansionist and guided by messianic ideology that the United States to resist. Truman read the events in the Mediterranean through Kennan's lens and assumed it justified a spirited response, even though Truman had made no official declaration of a "cold war" to this point. Stalin and Churchill had already made their Cold War declarations early in 1946, Truman rendered his own salvo in March 1947.

The Truman Doctrine argued that the world's future was split between totalitarianism and democracy. To preserve the American way of life, they would have to respond to Communist-inspired uprisings anywhere in the world. Funding the democratic forces in Greece was the first manifestation of this task; next, Truman requested a larger economic stimulus program for Western Europe that might rescue them from Communist subversion. His request became the European Recovery Program, or Marshall Plan, which the administration intended to supplement with the International Monetary Fund and the World Bank created at the Bretton Woods Conference of 1944. Next, Truman created the North Atlantic Treaty Organization (NATO), a vast military alliance premised upon multilateral response to Communist attack. The Marshall Plan and NATO gave Truman the tools for fighting the Cold War and promoting democratic capitalism in the Third World.

At home, Truman's anticommunist rhetoric energized a Republican Party resurgence. Midterm elections of 1946 ushered a new class of hawkish congressmen, the most notable were Wisconsin Senator Joseph McCarthy and



Training Center One, a secret CIA guerrilla warfare training base at Ft. Benning, Georgia, in 1951, where some members of the Air Supply and Communication Service (ARC) trained before going overseas. China had discovered that the newly created Central Intelligence Agency and the Air Force were collaborating on a new Cold War weapon, an "unconventional warfare" group whose connection to the CIA remains an official government secret. AP/WIDE WORLD PHOTOS.

California Congressman Richard M. Nixon, who defined themselves as Cold War activists. Republicans accused the Democratic Party with compromising America's post-war ambitions, giving Russia advantage in Western Europe. The capture of Russian spy of Klaus Fuchs in Great Britain, and then American counterparts Ethel and Julius Rosenberg, convicted for selling atomic secrets to the Soviet Union, along with the Alger Hiss case, validated Republican claims for many. Further proof came with the Soviet detonation of a nuclear device in 1949, and victory of Mao Tse Tung in China.

George Kennan again proved a useful guide for Truman with his *Foreign Affairs* article published July 1947 under the pseudonym Mister X. In the X Article, titled "The Sources of Soviet Conduct," Kennan warned that Russia operated on a mechanistic and fanatical faith that America had to meet wherever possible. The Soviet system, he advised, suffered from internal contradictions that would destroy it from within if given exposure. Truman and his secretary of state, Dean Acheson, interpreted Kennan's argument as "containment" and constructed the domestic tools for its execution. That July, Truman presented Congress with the National Security Act, which restructured the military establishment creating the Department of Defense, the National Security Council, and the CIA. Soon thereafter, he created loyalty policies aimed at rooting out Communists in the government.

The preemptory steps were not enough to meet the myriad strategic and political crises of the Cold War; therefore the administration attempted to streamline America's response even more with the creation of National

Security Council Memorandum (NSC) 68. As the top-secret blueprint for fighting the Cold War, NSC 68 called for a massive increase in military appropriations, the creation of the enormously more powerful hydrogen bomb, and levying taxes on the American public to pay for the program. Congress was reluctant to appropriate the sums of money needed for the Cold War, so Truman needed a dramatic event to shake them from their parochialism. That event came when North Korea, a Communist nation, crossed 38th parallel and invaded its democratic counterpart South Korea on June 24, 1950.

The Korean conflict proved to be a double-edged sword for Truman; it provided him the public mandate to institutionalize the Cold War, but it also laid the seeds for the political undoing of the Democratic Party. The battle itself swung unevenly, with the North Koreans at first advancing southward, and then United Nations forces led by General Douglass MacArthur recapturing ground. The turning point in the conflict occurred when a "volunteer" force from China crossed the river separating Korea and China, and sent MacArthur's forces into retreat. The Chinese attack threatened war, but Truman decided to quell to situation for the sake of American lives and global peace. His decision placed him at odds with MacArthur, which resulted in a war of words that ended with Truman unceremoniously removing the general from his command.

The Korean War, however, justified NSC 68 and a stronger stance in East Asia. Aside from the decision to support the South Koreans financially and militarily, Truman used it as a vehicle for funding the French colonial



An electromagnetic separation facility in Sverdlovsk, Russia, used for uranium enrichment, is shown in an undated high-altitude photograph taken during the Cold War. Many of the spy photos made of the Soviet Union taken in the urgent context of the Cold War now aid in peaceful purposes, such as disarmament verification. AP/WIDE WORLD PHOTOS.

war against the Vietnamese. Additionally, he created a military alliance for East Asia, the Australia, New Zealand, and United States (ANZUS) pact, and began rearming Germany as a buffer to Soviet advances west.

Domestic politics could not escape the gravitational pull of the Cold War, and its questions particularly burdened the presidential election of 1952. Red-baiters in the Republican Party, most notably Wisconsin Senator Joseph McCarthy, created such a relentless and fantastic attack on Truman's handling that it implicated the entire Democratic Party. The Republican candidate, Dwight Eisenhower (referred to as Ike), stayed above the fray, and allowed his reputation as the great general of World War II's European theater to win him the White House. Eisenhower took a pragmatic approach to the Cold War, and established the tradition that would remain in place until its end.

The death of Soviet Premier Joseph Stalin in March 1953 cast a shroud of uncertainty over Eisenhower's first year as president. Undeterred, however, he began defusing the anxious economy and international policies that dominated Truman's administration, with his "New Look" program. The New Look consisted of nuclear deterrence, designated by what his secretary of state John Foster Dulles called brinkmanship, massive relation, nation building in the Third World, the diffusion of American culture internationally, and a heavy investment in technological innovation. Eisenhower detested wasteful spending and

thought a combination of brinkmanship, technological innovation, and massive retaliation would streamline the military, yet preserve the nation's ability to respond quickly to crisis. Eisenhower gauged success in the Cold War effort broadly, thereby making the household washing machine as important in the Cold War arsenal as the B-52. In 1959, this correlation sparked the famous "kitchen debate" between Vice President Richard Nixon and Soviet Premier Nikita Khrushchev at the American National Exhibition in Moscow over which political economy promoted the better home life. As Eisenhower eschewed Truman's containment program for a policy of rolling back Communist expansion, reducing the size of conventional forces meant that the administration had to rely on the CIA to keep order in the Third World through counterintelligence and espionage.

International crises in Iran, Guatemala, and off the coast of mainland China tested Eisenhower's New Look early in his administration. Nationalist leaders in Iran and Guatemala assumed power in an attempt to redress grave social and economic inequalities in their countries, forcing the United States to respond. Although the Cold War implications were not necessarily apparent, America gained access to one of the world's largest oil depository by returning the Shah of Iran to power, and defeating the Arbenz regime guaranteed American businesses open access to the resources of Guatemala. The marriage of





U.S. Army tanks at Checkpoint Charlie, foreground, face Soviet Army tanks in 1961 during the most dangerous of several crises at the Friedrichstrasse checkpoint in Berlin during the Cold War. AP/WIDE WORLD PHOTOS.

Cold War politics and market concerns became a signature attribute of the New Look.

The Tachen Straits crisis presented a different problem. In 1954, mainland China began shelling two of the islands that neighbored Chiang Kai-Shek's Taiwan, Matsu and Quemoy with the threat that it was the start of a full-scale invasion to repatriate its citizens. To the surprise of the entire world, Eisenhower threatened the use of nuclear weapons to defend Taiwan unless China stopped the bombardment. Frightened by the possibility of nuclear calamity, neighboring countries India and Pakistan pressured China to desist, and the Tachen Straits crisis came to an uneasy end. The conflict, however, was a coarse example of brinkmanship and a precursor to America's deepening involvement in East Asia under the auspices of the "domino theory" of foreign policy. The image of Asian democracies, falling like dominos in rapid succession to nationalist or Communist infiltration, justified a greater presence in conflict between France and Vietnam.

Vietnam became a crisis for the United States at the Geneva Conference of 1954, when it was learned the French were on the verge of collapse in the region, signified by their surrender at Dienbienphu. To preserve democracy in Southeast Asia, the United States urged the division of Vietnam at the 17th parallel on the promise the country would have open elections within two years. In an attempt to thwart a potential Communist takeover in the upcoming elections, America installed Ngo Dinh Diem as South Vietnam's prime minister. Additionally, Eisenhower created a regional defense apparatus, the Southeast Asian Treaty Organization (SEATO), modeled after NATO, to protect the new nation as it bloomed into an independent state. Diem was an archconservative with autocratic tendencies who soon declared South Vietnam an independent state and cancelled the scheduled national elections. The United States supplemented Diem with vast amounts of capital, goods, machinery, weaponry, and advisors to train his soldiers. This effort marked the nation-building phase of the Cold War. The decision to build a nation as a response to what was essentially a civil war, committed the United States to the success and failure of South Vietnam, and would have dire consequences for America's place in the Cold War.

The Middle East became bothersome for Eisenhower in the later years of his administration, forcing him to make his own Cold War declaration in 1957. Egyptian president, Gamal Nassar created the Baghdad Pact, a military alliance between Egypt, Iraq, Iran, Pakistan, and Turkey in 1955 with the belief they could exploit the Cold War division for the benefit of Arab and Muslim nations. As part of his "middle road" strategy, Nassar opened relations with communist nations, Czechoslovakia and China, which soured America's attitude toward Egypt and compelled Dulles to cancel funds for the Aswan hydroelectric dam. Nassar responded by nationalizing the Suez Canal and assuming control of the oil traveling into the Mediterranean from the East. The situation escalated when Israel attacked Egypt over disputed territory, and Great

Britain and France took that as an opening to seize the Suez Canal. The conflict placed the world oil trade and Middle Eastern stability in jeopardy, and forced Eisenhower to pressure the European nations to relinquish control of the canal. Although resolved, the specter of Soviet influence in the oil-bearing region forced Eisenhower to take a stronger stand in the Middle East. The concern culminated in the "Eisenhower Doctrine," which held that the United States defend any Middle Eastern nation against communism. Eisenhower invoked the doctrine only twice, in the Jordanian uprising that spring and Lebanon in 1958, but it set precedence for future presidents Lyndon Johnson, Richard Nixon, and Jimmy Carter.

By the end of his term as president, Eisenhower faced ironic opposition. His administration privileged modernization, and ended under the suspicion of technological backwardness. Eisenhower created the National Aeronautics and Space Administration (NASA), and began America's reach for the heavens. The Russian launch of Sputnik, the unmanned satellite in late 1957, and the downing of the American U2 surveillance plane in 1960, demanded a greater investment in science and technology. John F. Kennedy drew upon this anxiety when he argued that America lagged behind the Soviet Union in missile production. The Missile Gap critique helped Kennedy capture the White House, but it also placed unrealistic burdens on the way he and his successor Lyndon B. Johnson conducted the Cold War.

In the 1960s, the Vietnam conflict pervaded America's Cold War politics. The decade began with President Kennedy suffering profound Cold War failures, the failed attempted overthrow of Cuba's Communist leader Fidel Castro at the Bay of Pigs, the CIA-sponsored assassination of Congolese Prime Minister Patrice Lumumba, the Cuban Missile Crisis, and the construction of the Berlin Wall. Needing to silence critics, Kennedy decided to take a more rigid stand against the Communists in South Vietnam. With Diem's popularity at a nadir due to his oppressive policies, Kennedy signed off on a plan to depose him. During the junta, however, the operatives assassinated Diem, foreshadowing Kennedy's own murder three weeks later.

When Lyndon B. Johnson assumed the presidency, he inherited the burden of not losing the Cold War in Vietnam. Weighted by fluctuations in the civil rights movement and burgeoning antiwar sentiment, Johnson accelerated both nation building in South Vietnam and military resistance to Communists. The entire conflict, and to some degree American prestige, came crashing to the ground in 1968 when Communist forces launched a massive attack against American and South Vietnamese forces in the major cities. Although the siege only had temporary success, it had a leveling effect on domestic sentiment. Cold War arguments carried less significance and the trouble became finding a way out. That responsibility fell to Richard Nixon who inherited the Vietnam and the Cold War in 1969.



In the midst of the conflict, Nixon and his secretary of state, Henry Kissinger, began to redefine the Cold War into a mutual understanding of the boundaries between the U.S. and Russia. He coupled this with the Nixon Doctrine, which held that America would relinquish some of its military commitments. Breaking precedent, Nixon went to China and began arms reduction talks, or *détente*, with the Russians. To counter his critics, Nixon coupled *détente* with a brinkmanship-like tactic he called the “mad man theory.” According to this strategy, American allies would warn Third World nationalists that Nixon was insane and willing to use nuclear weapons to end disputes. The crazy man tactic had little to no effect on its intended audience, North Vietnam, or any of the other Cold War dissidents. Nixon’s Strategic Arms Limitation Talks (SALT I), begun in 1969 and concluded May 1972, between the United States and Brezhnev regime exemplified the spirit his doctrine. While SALT I failed to reduce the creation and stockpiling of new, more destructive weapons, it was a progressive gesture toward an international dialogue on nuclear weapons.

Buoyed by the apparent success of *détente* and the belief that China could help end the war in Vietnam, Nixon went into the presidential election of 1972 confident in his Cold War program. Indeed, twenty-five years had shifted the Cold War from security concerns, to a contest of development, to Nixon’s program of limited contact, and ended the 1960s with the possibility of an uneasy coexistence between Soviet socialism and democratic capitalism. Many questions were still unanswered regarding the conflict in Vietnam, rising nationalism in the Middle East, the global economy, domestic dissent, and nuclear control. These issues would dominate the last seventeen years of the Cold War.

#### ■ FURTHER READING:

##### BOOKS:

- Gaddis, John Lewis. *We Now Know: Rethinking Cold War History*. Oxford University Press, 1998.
- La Feber, Walter. *America, Russia, and the Cold War*. McGraw-Hill Humanities, 2001.
- McDougall, Walter. *The Heavens and the Earth: A Political History of the Space Race*. Baltimore: Johns Hopkins University Press, 1997.
- McMahon, Rober. *The Cold War on the Periphery*. New York, Columbia University Press, 1994.
- Wagnleitner, Reinhold. *Cocacolonization and the Cold War*. Chapel Hill, The University of North Carolina Press, 1997.

##### PERIODICALS:

- Frank Costigliola, “Unceasing Penetration”: Gender, Pathology, and Emotion in George Kennan’s Formation of the Cold War.” *Journal of American History* 83 (March, 1997): 1309–1939.

##### SEE ALSO

*Berlin Airlift*

*CIA (United States Central Intelligence Agency)*  
*Cold War (1945–1950), The Start of the Atomic Age*  
*Cold War (1972–1989): The Collapse of the Soviet Union*  
*National Security Act (1947)*  
*NATO (North Atlantic Treaty Organization)*  
*NSC (National Security Council)*  
*Nuclear Reactors*  
*OSS (United States Office of Strategic Services)*  
*Truman Administration (1945–1953), United States National Security Policy*  
*United States, Intelligence and Security*

## Cold War (1972–1989): The Collapse of the Soviet Union

■ JOSEPH PATTERSON HYDER

By the early 1970s, the Soviet Union was at the peak of its power. The Communist Party remained the sole political force in the Soviet Union, but decades of post-Stalinist economic reforms left the Soviet empire with a seemingly robust economy and an increased standard of living for Soviet citizens. Wages in the Soviet Union increased sharply. The Soviet Union was the world’s leading producer of steel and oil. Urban dwellers enjoyed modern appliances, such as televisions and dishwashers, and lived mostly in the plentiful newly-constructed single-family apartments.

In addition to these economic advantages at home, the Soviet Union attempted to assert itself as the world’s dominant superpower. For nearly every Soviet success in the early 1970s, the United States suffered a setback. While the oil-rich Soviet economy continued to grow, the economy of the United States strained under the pressure of the OPEC imposed oil embargo of 1972 and 1973.

The Soviet Union also prevailed on the international stage. Soviet-backed North Vietnamese forces expelled American troops after a prolonged conflict. The communist victory in Vietnam, coupled with U.S. public opposition to the conflict, signaled an end to the American policy of communist containment in Southeast Asia. With further containment of communism in doubt, the United States had to reposition itself on the international scene. The administration of President Richard M. Nixon embarked on a policy of *détente* with China, culminating with Nixon’s trip to China, and, to some degree, with the Soviet Union. The pace of Soviet nuclear weapon production greatly alarmed Washington. Fearing a Soviet advantage in the arms race, Nixon signed the Strategic Arms Limitations Talks (SALT I).

In addition to Southeast Asia, Soviet ideology was gaining support in other parts of the world, including Latin America. Soviet-supported troops in Central and South America alarmed American officials, who feared communist expansion in the Western Hemisphere. Still deeply



Berliners sing and dance on top of the Berlin Wall in front of the Brandenburg Gate to celebrate the opening of East-West borders in 1989. Built of barbed wire and concrete in 1961, the wall divided Berlin and became the most powerful symbol of the Cold War. AP/WIDE WORLD PHOTOS.

wounded by opposition to the Vietnam War, however, America resorted to conducting covert operations in Latin America. During the administration of President James E. Carter, communist backed Sandinistas overthrew Nicaragua's government. President Ronald Reagan later provided financial and material support to anti-Sandinista rebels. Reagan also backed anti-communist forces in El Salvador, even though Congress did not always agree with the White House on the issue of Nicaragua and El Salvador.

With proxy victories in Southeast Asia and Latin America and with a booming national economy, the power of the Soviet Union appeared formidable under Soviet Premier Leonid Brezhnev. To many outside observers, the Soviet Union appeared to be on the verge of winning the Cold War. The post-Brezhnev years, however, would see the internal collapse of the Soviet Union. Even while the Soviet Union was soaring to new heights, cracks were beginning to form in the monolithic empire. Economic troubles, military failures, and emerging nationalism would soon result in the end of the Soviet Union and communist regimes in Eastern Europe.

**Economic stagnation and the arms race.** The vigorous Soviet economy of the late-1960s and early 1970s quickly

fell victim to the very factors that had contributed to its success, central planning and raw materials allocation. Brezhnev recognized that the Soviet economy was slowing, and attempted to patch problems rather than completely overhaul the system. His efforts failed. Even if Brezhnev had attempted to overhaul the Soviet economy, the highly entrenched special interests that made their living by manipulating the Soviet Union's centrally planned economy could have defeated Brezhnev's efforts.

Throughout the 1970s and into the mid-1980s, the Soviet Union's GNP and industrial output continued to increase, but at a lessening pace, eventually leading to economic stagnation. The Ninth Five Year Plan (1970–1975) saw a growth rate of approximately 3%. The period of 1975–1980 experienced a growth rate of between 1% and 1.9%, depending on whether revised Soviet numbers or the West's estimate is examined. Likewise, 1980–1985 saw a further decline in economic growth, between 0.6% and 1.8%. Declining economic growth rates were not confined to the Soviet Union. Eastern Europe, with its economies intertwined with the Soviet Union's, suffered a similar fate.

This declining growth rate in the 1970s and 1980s resulted in the Soviet Union receiving a diminishing rate of return on capital investment. This proved disastrous for the Soviet economy, because by 1980, the Soviet Union

was spending nearly one-third of its GNP on capital investment, with most of the sum dedicated to the military. The military was consuming such a large portion of the Soviet economy for two reasons: the Soviet involvement in Afghanistan and the arms race with the United States. These two events would weigh heavily in the Soviet economic demise and lead to its inevitable fall. A weak economy prevented the Soviet Union from reacting appropriately to each experience.

The stagnant Soviet economy of the 1970s would have fared far worse had it not been for vast oil and natural gas production propping up the economy. By the late 1970s, technological backwardness and poor management under the centrally planned Soviet economy resulted in depleted oil and gas reserves. This led Brezhnev to turn his eye towards the oil and gas reserves of Central Asia. Afghanistan had long been a relatively undeveloped country comprised of numerous semi-autonomous ethnic groups. Brezhnev assumed that the Soviet Union could achieve a quick and decisive victory over the country and expand its influence of Communism into Central Asia.

The United States and the rest of the world quickly condemned the Soviet invasion of Afghanistan in 1979. The United States also provided covert support to the mujahideen, or Afghani resistance fighters. Rapid turnover in Soviet leadership following the death of Brezhnev in 1982 also hampered the war effort. The short-lived regimes of Yuri Andropov and Konstantin Chernenko provided for an inconsistent Afghan policy. The Soviet military operation quickly bogged down and faced stiff resistance in the harsh terrain of Afghanistan.

The Soviets erroneously assumed that since the Afghans were economically disadvantaged, they would be quickly defeated and embrace communism. The opposite result happened. As the Afghans had little to lose by continuing to fight, instead of driving Afghanistan to communism, the Soviet invasion forged the Afghani Islamic resistance. A decade after the invasion, Soviet troops withdrew.

The war in Afghanistan had an even more adverse effect on the Soviet Union than the Vietnam War had on the United States. Thousands of Soviet troops died in a conflict that resulted in the defeat of a superpower by a developing country. Moreover, the conflict strained an already weak economy. The conflict angered Soviet citizens, and they began demanding accountability from the state. Brezhnev and his successors intended the war in Afghanistan to reassert the supremacy of the Soviet Union. Instead, the conflict proved that the superpower's might was waning.

The war in Afghanistan also distracted the Soviet Union from its arms race with the United States, thus allowing America to gain a technological advantage. The United States ratcheted up pressure on the U.S.S.R. through several means. The Reagan administration began placing missiles in Western Europe, primarily in Western Germany, strategically located to intimidate Eastern Europe

and the Soviet Union. Reagan also began building up the U.S. military. Reagan commissioned new aircraft carriers and expanded America's stealth aircraft program. To the Soviets, these actions signaled a widening weapons gap, particularly in terms of technologically advanced weapons.

Perhaps the greatest threat to the Soviet Union was the United States' Strategic Defense Initiative (SDI), also known conventionally as Star Wars. The SDI was a planned satellite based weapons system that would detect and destroy missiles fired at the United States. Such a technological advancement would have rendered Soviet ICBMs useless. The Soviet Union tried to dissuade the United States from implementing the SDI, but the Reagan administration refused to back away from the proposal. In reality, the SDI was only in the technological planning stages; the Soviets, however, bought America's bluff, prompting a quick and expensive advance in their lagging military technology. This increased spending further accelerated the Soviet economic decline.

Realizing a weapons gap, the Soviet Union began pushing the Reagan administration for nuclear arms talks following the death of Brezhnev in 1982. The U.S. soon entered negotiations over the Strategic Arms Reduction Treaty (START). However, numerous changes in post-Brezhnev Soviet leadership, Solidarity strikes in Poland, and other issues prevented the completion of the START during the Reagan administration.

**Gorbachev and the end of the Cold War.** After a decade of over-inflated military expenditures, dwindling oil revenue, and a centrally-planned economy that was too rigid to adapt to consumer demands, Mikhail Gorbachev, upon assuming office, declared the Soviet economy to be in a "pre-crisis." Gorbachev immediately transformed the face of Soviet politics. Gorbachev quickly appointed new members to the Politburo and Secretariat, ridding each of many hardline, longtime bureaucrats. Gorbachev also attempted to reform the KGB, replacing many agents and bureaucrats. Despite the shake-up, the KGB's operational power emerged from Gorbachev's early reforms relatively unscathed.

After reforming the government, Gorbachev set out to reform the economy and ultimately, Soviet society. Gorbachev's economic reforms (*perestroika*, or restructuring), were perceived as noble, but poorly executed. The Twelfth Five Year Plan tried ambitiously and quickly to reform the Soviet economy. Gorbachev sought to update industrial equipment and computer systems, while simultaneously expecting workers to produce higher quality products in greater quantities. Gorbachev also tried to decentralize the economy by giving different regions greater control over industry. All of these goals proved to be unrealistic given Gorbachev's timetable to dismantle the gargantuan Soviet bureaucracy in favor of a more streamlined and efficient system.

By 1986, Gorbachev also began experimenting with the notion that greater democracy, if presented in the

proper format, would lead to increased socialism. Gorbachev wanted to strip away Stalinism and its accompanying bureaucracy and return to the communism of Lenin. Initially, Gorbachev underestimated the effect that allowing Soviet citizens to question the past, in particular the brutality of Stalin, would have upon the citizenry, leading them to follow their lines of questioning up to the present day. Soon, however, Gorbachev came to accept and embrace the concept that he termed *glasnost*, or “openness.”

Glasnost initially allowed only the divulgence of information by the state. Gorbachev held that if the Soviet Union was more open and honest about its past, then Soviet and Eastern European citizens would be more likely to follow Gorbachev’s economic lead. Even a large number of bureaucrats in the KGB supported glasnost. The KGB’s information network had become burdened and as ineffective as the bureaucracy that it supported. Therefore, many KGB officials assumed that fostering an atmosphere of openness would result in new and better informants.

Although Gorbachev intended glasnost to strengthen the communist regime, he did not initiate a crack-down when Soviet citizens went beyond the original intent of glasnost. Soviet intellectuals began questioning the very tenets of Soviet Communism and attacked the Communist Party in newspapers, journals, film, and books. Eastern European thinkers followed the lead of their Soviet counterparts.

Consequently, glasnost had the unintended effect of spurring nationalist and anti-communist movements in Eastern Europe and the Soviet republics. Dissidents in Poland, East Germany, Czechoslovakia, and other Soviet-satellite states staged labor demonstrations. Citizens took to the streets, demanding that the Communist Party step aside and allow democratic elections. In fall 1989, the Berlin Wall, long a symbol of the division between Eastern Europe and the world, fell, allowing East and West Berliners to cross freely. The Communist Party and its East Germany secret police organization, the Stasi, had lost power. Within months of the fall of the Berlin Wall, other Eastern European countries broke away from Moscow’s influence and expelled their communist leaders. With the exception of Romania, most of the revolutions of 1989 and early 1990 were relatively peaceful.

In the wake of the Eastern European revolts and the euphoria that followed, the Soviet Union had little choice but to allow greater freedoms. In February, 1990, the Communist Party agreed to relinquish its political monopoly. Many of the civic groups that had been voicing displeasure with the Soviet system formed political parties. Most of these new parties, especially those outside of Russia had a nationalist agenda. Within a month, the Baltic republic of Lithuania declared itself an independent state. Other Soviet republics quickly followed.

In June 1991, Gorbachev allowed free elections to choose a president of the Russian Republic. Boris Yeltsin,

a former Gorbachev-supporter, won a landslide victory over Gorbachev’s chosen candidate. In August, 1991, a group of communists hardliners attempted a poorly organized coup while Gorbachev was on vacation at the Black Sea. The coup failed, and strengthened Boris Yeltsin, the primary target of the coup. The coup also undermined the leadership of Gorbachev, who continued to govern ineffectively until his resignation on December 25, 1991. The following day, the Supreme Soviet officially declared an end to the Soviet Union.

#### ■ FURTHER READING:

##### BOOKS:

- Baucom, Donald. *The Origins of SDI*. Lawrence, KS: University Press of Kansas, 1992.
- Brown, Archie. *The Gorbachev Factor*. Oxford: Oxford University Press, 1997.
- Colton, Timothy, and Robert Legvold. *After the Soviet Union*. New York: W. W. Norton, 1992.
- McGuire, Michael. *Perestroika and Soviet National Security*. Washington, D.C.: Brookings Institute, 1991.
- McMahon, Robert. *The Cold War on the Periphery*. New York: Columbia University Press, 1994.

##### SEE ALSO

- Carter Administration (1977–1981), United States National Security Policy*
- Cold War (1945–1950), The Start of the Atomic Age*
- Cold War (1950–1972)*
- Ford Administration (1974–1977), United States National Security Policy*
- KGB (Komitet Gosudarstvennoi Bezopasnosti, USSR Committee of State Security)*
- Nixon Administration (1969–1974), United States National Security Policy*
- Reagan Administration (1981–1989), United States National Security Policy*

---

## Colombia, Intelligence and Security

---

Colombia emerged as an independent nation in 1830, following the collapse of Spanish rule in the region, then known as Gran Colombia. Large-landowning and military interests alternately dominated the nation’s politics, causing long-standing political tension. In the 1960s, political extremists and paramilitary insurgent groups began attacking government interests in the capital. The conflict escalated in the 1990s, destabilizing the Colombian government and allowing areas of the countryside to fall to

guerilla control. Violence and sporadic fighting continue to be endemic in the nation, but the government restructured intelligence, police, and military forces to combat the problem.

Colombia's main intelligence service is the National Intelligence Service (SIN). The SIN coordinates civilian intelligence efforts, including those of subsidiary departments such as counter-intelligence, anti-terrorism, and surveillance forces. SIN operations cover both domestic and foreign intelligence, but focus on combating political insurgency and threats to national security. The agency works with the Colombian National Police to investigate criminal activities related to drug cartels or paramilitary groups, as well as instances of government corruption.

The Department of Administrative Security (DAS) works to protect government officials and buildings. The DAS also conducts limited counter-espionage operations to ensure the safety and security of government information and communication systems.

Military intelligence in Colombia is the responsibility of the army and the Intelligence Department (F-2). Military intelligence assesses external threats to Colombian national security, and conducts surveillance of paramilitary and rebel groups within national borders.

After a series of constitutional reforms in the early 1990s, the Colombian government began negotiations with leftist rebel and right-wing paramilitary groups. The government in Bogotá ceded control of some remote areas to opposition control, but the transfers of power did little to abate continued violence. The government continues to use intelligence and security forces for both anti-paramilitary operations and political espionage with some success. Creation of the Anti-Kidnapping Squad has reduced the number of government officials, journalists, and foreign businesspeople taken by insurgent forces who seek to intimidate the government or extract ransom payments.

In the midst of political chaos, the presence and influence of drug trafficking rings, cartels, and crime syndicates has increased in Colombia and throughout the surrounding region. The Colombian government has pledged support to international efforts to reduce the cultivation, production, and trafficking of illicit drugs. With the aid of the United States, and other nations, Colombia patrols its countryside with aerial surveillance, has implemented tighter security in its ports, and begun a campaign to seize illegal funds and halt money laundering operations.

#### ■ FURTHER READING:

##### ELECTRONIC:

Central Intelligence Agency. "Colombia" CIA World Factbook <<http://www.cia.gov/cia/publications/factbook/geos/co.html>> (April 8, 2003).

## Colossus I

■ DAVID TULLOCH

Colossus I was the world's first programmable computer. Colossus I was created during World War II by the British to speed up the decryption of German messages encoded by the Lorenz Schlüsselzusatz (SZ) 40 and 42 machines.

In 1940, the British began to intercept German non-Morse teleprinter text that used the Baudot Code, an international standard where each letter is represented by five binary elements. In modern binary notation, A is 11000, B equals 10011, and G is 01011. The Lorenz machine used a code devised by Gilbert Vernam (1890–1960) in 1918. Obscuring letters were added in modulo 2 addition, where adding like to like gives a 0, while like and unlike equals 1.

The Lorenz machine added two obscuring letters generated by two sets of five-toothed wheels, and two motor wheels arranged in any order and starting position. The British did manage to break this system when multiple messages were sent using the same initial settings, but decoding was time-consuming and only partially successful. Eventually, the internal workings of the SZ machines were deduced, and allowed decoding, providing the starting position of the wheels could be found. Decoding by hand, however, took several weeks. Max Newman (1897–1984) used the ideas of Alan Turing (1912–1954) to design a machine to speed up the process. Called "Robinson" after Heath Robinson, the British cartoonist and designer of fantastic machines, it compared the coded text with another piece of tape that represented the Lorenz wheel settings. However, keeping the two paper tapes in sync at high speed was difficult, and they frequently tore.

Tommy Flowers (1905–1998), an engineer, had the idea of representing the Lorenz wheel settings electronically, doing away with the need for synchronised tapes. Despite many doubters, Flowers spent ten months building the Colossus Mark I, completed on December 8, 1943. Colossus contained 1500 valves, more than had been previously used in a single device, and used photocells to read punched paper tape at 5000 characters per second. It had a limited memory, of five-bits, and used pluggable logic gates. The wheel settings of the Lorenz ciphers were simulated in collections of thyratons, gas-filled triodes that acted as one-bit stores. The results were then printed via a typewriter.

The Colossus Mark I was quickly outdated by the Colossus II, the first of which was finished by June, 1944. Nine Mark IIs were built, and the original machine was upgraded to become the tenth machine, each one occupying a large room. The Colossus II used around 2500 valves and read the tape five times as fast as its predecessor.

The Colossus machines counted through the length of the encoded text many times, effectively trying out billions of combinations to determine which initial wheel

settings of the Lorenz encoder were statistically significant. The Colossus output did not give a decoded message, but rather the settings of the first set of five wheels. Humans, using a combination of statistics, language skills, and intuition did the remaining decoding. Finally, the complete wheel settings were fed into a device that produced the deciphered message. Later, the versatile Colossi were reprogrammed to do more of the code-breaking work, but there was always considerable input from their human operators.

Breaking the Lorenz cipher gained the Allies crucial information that aided in major operations, such as the Battle of Kursk, and the D-Day landings. Colossus showed that Turing's ideas of a universal computer could be made into practical machines. However, the existence of Colossus was kept secret for many years, and so the American Electronic Numerical Integrator and Computer (ENIAC), completed by the U.S. Army in 1946, was considered the world's first computer until information on Colossus was finally declassified in the 1970s. In 1996, a Colossus was reconstructed, and it can be seen at the Bletchley Park Museum.

#### ■ FURTHER READING:

##### BOOKS:

- Hinsley, F. H., et al. *British Intelligences in the Second World War: Its Influence on Strategy and Operations*, Volume Three, Part I. London: Her Majesty's Stationary Office, 1984.
- Sale, Anthony E. "The Colossus of Bletchley Park—The German Cipher System," in Raúl Rojas and Ulf Hashagen *The First Computers: History and Architectures*. Cambridge, MA: MIT Press, 2000.
- Smith, Michael. *Station X: The Codebreakers of Bletchley Park*. London: Channel 4 Books, 2000.

##### ELECTRONIC:

WWII Codes and Ciphers. <<http://www.codesandciphers.org.uk>> (December 19, 2002).

##### SEE ALSO

*Cipher Key*  
*Cipher Machines*  
*Codes and Ciphers*  
*Enigma*

## COMINT

### (Communications Intelligence)

#### ■ JUDSON KNIGHT

COMINT or communications intelligence is intelligence gained through the interception of foreign communications, excluding open radio and television broadcasts. It is

a subset of signals intelligence, or SIGINT, with the latter being understood as comprising COMINT and ELINT, electronic intelligence derived from non-communication electronic signals such as radar. During the early part of the modern intelligence era, the terms "signals intelligence" and "communications intelligence" were used virtually interchangeably, and therefore, much of what was described as signals intelligence in World War II is more properly understood as COMINT.

## Early History of Army and Navy COMINT

COMINT is the province of several services, both military and non-military, most notably the National Security Agency (NSA) and the United States Army Intelligence and Security Command (INSCOM). Until the establishment of NSA in 1947, however, the majority of COMINT took place under the aegis of "signals intelligence" activities in the two principal military services. Though military cryptanalytic and cryptographic operations dated back at least to World War I, and included activities at the War Department Military Intelligence Division under the direction of Herbert O. Yardley, the first true COMINT organization was the Army's Signal Intelligence Service (SIS).

Established on April 24, 1930, SIS not only undertook cryptographic and cryptanalytic tasks, but developed cipher machines and produced studies on cryptology. Its greatest achievement was its breaking of the Japanese diplomatic ciphers with the PURPLE code machine prior to World War II. In June 1942, after the outbreak of war, SIS acquired an intercept operation in the form of the 2nd Signal Service Battalion, which conducted radio intercepts at Vint Hill Farms in Warrenton, Virginia.

**A tale of two services.** The interaction of army and navy COMINT activities during the war is rather like a morality tale of two brothers, the older one highly favored, but failing to live up to expectations, and the younger one coming from behind to triumph. In this analogy, the army was the "older brother," and the navy, which lacked a true COMINT organization during the war, the surprising dark horse. After its initial victory with PURPLE, SIS conducted a long and frustrating effort to crack Japanese military codes, succeeding only in 1944.

The Navy had, at the end of World I, a cryptologic bureau that had emerged during the war. The bureau provided codes for the use of President Woodrow Wilson during the Paris Peace Conference, but when Yardley demonstrated his ability to break the naval codes, the Office of Naval Intelligence (ONI) closed down the cryptologic bureau in July 1918. Navy COMINT efforts then retreated to the shadows—a fitting place for intelligence operations.

**Naval successes in the 1920s.** Operating through the Research Desk at the Office of Naval Communications, the Navy's informal COMINT unit, designated OP-20-G, consisted of Lt. Laurence F. Safford and a four-person civilian staff. Denied any help from the army, the unit, which began operation in 1924, turned its attention to Japanese naval codes.

By then the navy, in collaboration with the Federal Bureau of Investigation and the New York City police, had already undertaken several attempts to—quite literally—steal codes from the Japanese Consulate in New York City. A series of breaks-in during the 1920s led to the compilation of a Japanese codebook. Because of the book's red binding, the code itself was thenceforth known as RED.

**COMINT cooperation during the war.** The navy actually played a critical role in decoding PURPLE: the machine that broke the code was constructed at the Washington Naval Yard in 1940. Thereafter SIS and the naval unit worked together to break the Japanese diplomatic code. At the same time, the navy had more success than the army in breaking the codes of its Japanese counterpart—but unfortunately, a change of code on December 1, 1941, helped make the United States vulnerable to the attack on Pearl Harbor that occurred six days later.

However, the navy was able to penetrate Japan's naval codes several other times, reacquiring them after changes by the Japanese, and thus contributed to American success in the battles of the Coral Sea and Midway in mid-1942. By the end of the war, the status of naval COMINT had risen to such a degree that SIS actively sought its help.

**The postwar era.** Between 1942 and September 1945, SIS went through a staggering number of name changes, to Signal Intelligence Service Division, Signal Security Division, Signal Security Branch, Signal Security Division (again), Signal Security Service, and Signal Security Agency. In September 1945, it became the Army Security Agency, which was replaced by the Army Intelligence and Security Command in January 1977.

The naval COMINT office only acquired a formal name in 1968, when it was designated the Naval Security Group. Later it was placed under NSA, which replaced the Armed Forces Security Agency, a shortlived (May 1949–October 1952) attempt to consolidate cryptology operations of all the services.



An E-3 Sentry airborne warning and control system aircraft (AWACS) lands at Kadena Air Base on Okinawa, Japan. ©REUTERS NEWMEDIA INC./CORBIS.

## ■ FURTHER READING:

### BOOKS:

- Aldrich, Richard J. *The Hidden Hand: Britain, America, and Cold War Secret Intelligence*. Woodstock, NY: Overlook Press, 2002.
- Alvarez, David J. *Allied and Axis Signals Intelligence in World War II*. Portland, OR: F. Cass, 1999.
- Andrew, Christopher M. *Codebreaking and Signals Intelligence*. Totowa, NJ: F. Cass, 1986.
- Bennett, Richard M. *Espionage: An Encyclopedia of Spies and Secrets*. London: Virgin Books, 2002.
- Gilbert, James L., and John Patrick Finnegan. *U.S. Army Signals Intelligence in World War II: A Documentary History*. Washington, D.C.: U.S. Government Printing Office, 1993.
- Richelson, Jeffrey T. *The U.S. Intelligence Community*, fourth edition. Boulder, CO: Westview Press, 1999.
- Sexton, Donal J. *Signals Intelligence in World War II: A Research Guide*. Westport, CT: Greenwood Press, 1996.
- West, Nigel. *The SIGINT Secrets: The Signals Intelligence War, 1900 to Today: Including the Persecution of Gordon Welchman*. New York: W. Morrow, 1988.

### ELECTRONIC:

- Pearl Harbor Revisited: U.S. Navy Communications Intelligence, 1924–1941. U.S. Naval Historical Center. <<http://www.history.navy.mil/books/comint/>> (March 29, 2003).

### SEE ALSO

- Army Security Agency*  
*Cryptology, History*  
*INSCOM (United States Army Intelligence and Security Command)*  
*Intelligence*  
*NMIC (National Maritime Intelligence Center)*  
*NSA (United States National Security Agency)*  
*SIGINT (Signals Intelligence)*

## Commerce Department Intelligence and Security Responsibilities, United States

### ■ JUDSON KNIGHT

In addition to promoting trade and industry, the United States Department of Commerce (DOC), through its various bureaus, conducts the census, maintains standards of weights and measures, and monitors the oceans and atmosphere. The department has a number of intelligence and security functions, ranging from protecting computers against hackers to overseeing exports of suspicious transfers to hostile nations.



A section of structural steel beam recovered from the World Trade Center hovers over members of the media during a 2002 press conference at the Commerce Department's National Institute of Standards and Technology. A 24-month study was announced to examine the structural failure and collapse of the WTC buildings during the terrorist attacks of September 11, 2001. AP/WIDE WORLD PHOTOS.

Founded in 1903 as the Department of Commerce and Labor, the Department of Commerce emerged in its present form after the Department of Labor separated from it in 1913. The modern Commerce Department includes, among other offices, the bureaus described briefly below.

The Economics and Statistics Administration (ESA) is responsible for compiling, analyzing, and producing reports based on economic and demographic data. Similar in mission is the Bureau of Economic Analysis (BEA), which is dedicated to collecting statistical information with the aim of producing an accurate picture of the U.S. economy. Closely related to ESA and BEA is one of the most well known sections of Commerce, the Bureau of the Census. In addition to the decennial (once every decade) census, the Census Bureau conducts demographic and



economic censuses, and produces more than 200 annual surveys, many for other government agencies.

At the center of the traditional Commerce Department mission are three bureaus. The International Trade Association (ITA) promotes U.S. exports of manufactured goods, nonagricultural commodities, and services. Assisting minorities and the economically disadvantaged are the Minority Business Development Agency (MBDA) and the Economic Development Administration (EDA). The first of these promotes minority-owned business, while the EDA helps economically distressed communities by providing grants, assisting in job retention, and stimulating industrial and commercial growth within these communities.

**Science, technology, and national security.** Commerce bureaus with a special scientific focus include the National Institute of Standards and Technology (NIST, covered elsewhere) and the National Oceanic and Atmospheric Administration (NOAA). NOAA is concerned with environmental assessment and prediction, protection of public safety, weather forecasting, and the protection of marine resources.

In the area of technology are three other bureaus: the National Telecommunications and Information Administration (NTIA), the Patent and Trademark Office (PTO), and the Technology Administration (TA). NTIA acts as the principal advisor to the president on matters of telecommunications policy with regard to economic and technological advancement, as well as regulation. It is one of several government agencies concerned with the operation of the Internet. Like the Census Bureau, PTO is another office of the Commerce Department whose functions are well known; not only does it serve as a registry for new inventions and processes, it acts to protect this information, and to promote innovation. As for TA, it is concerned with promoting the economic competitiveness of U.S. technology companies.

The Bureau of Industry and Security (BIS) is concerned with issues of national security, including efforts to stop the proliferation of weapons of mass destruction. At the same time—and in a function more commonly associated with the Commerce Department in the popular imagination—BIS also seeks to further the growth of U.S. exports.

**Other intelligence and security matters.** Most of the above-named bureaus fall under one of a half-dozen Commerce undersecretaries. In addition, other offices are directed by officials, among them the General Counsel, who report directly to the Secretary of Commerce. Furthermore, a presidential directive in 1998 placed the Critical Infrastructure Assurance Office (CIAO; see entry) under the Commerce Secretary's direction without establishing an obvious chain of command.

Among the Commerce offices involved in intelligence functions are the Office of Executive Support (OES, formerly the Office of Intelligence Liaison), which reports to the General Counsel; the Office of Export Enforcement (OEE), which reports to the undersecretary for international trade; and the Office of Foreign Accountability (OFA), whose leadership comes from the assistant secretary for export administration.

OES, as its old name (changed in 1996) made clearer, serves as a liaison between the Commerce Secretary and the intelligence community, especially where technology transfer issues are concerned. OEE oversees the export of sensitive technology, and continually monitors trade data with an eye toward national security. As for OFA, during the Cold War, its task was to promote advantages for U.S. companies competing against Soviet and Chinese exports. Since the early 1990s, however, it has been more concerned with the proliferation of nuclear and ballistic missile technology, as well as with chemical and biological weapons.

Under the administration of President William J. Clinton, the Commerce Department became an area of security concern. These issues first emerged when Ron Brown, Clinton's first Secretary of Commerce, was reported to be packing overseas trade missions with high-volume donors to the Democratic Party. Later, Clinton replaced Brown (who died in a 1996 plane crash) with William Daley, but more problems emerged with revelations that Deputy Assistant Secretary for Trade Missions John Huang had obtained a high-level security clearance while maintaining close contact with the Chinese government. In February 1998, Daley announced plans to tighten security and limit access to classified information within the department.

#### ■ FURTHER READING:

##### BOOKS:

Bowers, Helen. *From Lighthouses to Laserbeams: A History of the U.S. Department of Commerce*. Washington, D.C.: U.S. Department of Commerce, 1995.

##### PERIODICALS:

White, Ben. "Commerce Secretary Unveils New Security Policy." *Washington Post* (February 11, 1998): A19.

##### ELECTRONIC:

Department of Commerce. <<http://www.commerce.gov>> (January 28, 2003).

##### SEE ALSO

*Clinton Administration (1993–1997), United States National Security Policy*  
*Critical Infrastructure Assurance Office (CIAO), United States*  
*NIST (United States National Institute of Standards and Technology)*  
*Port Security*  
*Satellite Technology Exports to the People's Republic of China (PRC)*



Elsie Meeks, the first American Indian member of the U.S. Commission on Civil Rights, in her Kyle, South Dakota office in 2001. AP/WIDE WORLD PHOTOS.

## Commission on Civil Rights, United States

■ JUDSON KNIGHT

Established under the Civil Rights Act of 1957, the United States Commission on Civil Rights serves in an investigative, fact-finding role with regard to allegations of discrimination or denial of equal protection under the laws. The commission, as it is known, has no enforcement powers, but works closely with the federal, state, and local agencies that have powers of enforcement.

Unlike a number of federal agencies whose upper echelons consist almost exclusively of appointees chosen by the current administration, the commission is designed to be independent. Four of its eight members are appointed by the president, but the presence of persons who would likely be friendly to the administration is counterbalanced in large degree by the other half of the commission, whose members are appointed by Congress.

It is significant that the commission began life at a time when both houses of Congress were dominated by Democrats, while Dwight D. Eisenhower, a Republican,

held the White House—an ideal situation for a politically diverse Commission. Though the years since have seen long periods in which Democrats controlled both the executive and legislative branches (1961–69, 1977–81, 1993–95), as well as a brief period in 2001 when Republicans enjoyed the same advantage, differences between White House, Senate, and House leaders have helped to ensure a healthy degree of political diversity on the Commission. Furthermore, its rules hold that no more than four members at any one time shall be of the same political party.

**Political independence.** Although the president appoints the chairperson and vice-chairperson, one incident from the administration of George W. Bush serves to illustrate the commission's independence from the Chief Executive. The commission ordered a study of the controversial November 2000 balloting in Florida, which resulted in a deadlock between then-Governor Bush and his Democratic opponent, Vice President Albert Gore, Jr. Ultimately the United States Supreme Court declared Bush the victor, but only after five weeks of bitter legal wrangling. The commission concluded in June 2001, by a vote of 6–2, that the voting in Florida had been characterized by “injustice, ineptitude, and inefficiency” that resulted in the loss of some voting rights by minority participants in the election.

The conclusion, which the two dissenting board members described as based on faulty analysis, resulted from findings that minority voters' ballots were more likely to be rejected than those of their white counterparts.

**Responsibilities and powers of the commission.** The Florida study is an example of the commission fulfilling one aspect of its mandate: investigation of allegations that citizens have been denied their right to vote either by fraudulent practices, or by reason of their race, color, sex, religion, age, disability, or national origin. The commission also studies and compiles information regarding discrimination or denial of equal protection in the administration of justice, or because of race and the other characteristics named previously. It submits reports and recommendations to the White House and Congress, and issues public service announcements designed to discourage discrimination or the denial of equal protection under the law.

The commissioners, who serve six-year terms, meet on a monthly basis, except during August, and meet several other times each year to hold hearings, conferences, consultations, or briefings. In the process of producing documents, the commission can call witnesses and issue subpoenas within a state at which a hearing is held, and within a 100-mile radius of the site of the hearing, whichever is larger. The commission maintains advisory committees at the state level, and refers the many complaints it receives to appropriate federal, state, or local agencies (including ones concerned with law enforcement), as well as private organizations.

The results of commission studies usually see publication, and the commission produces a number of pamphlets on a yearly basis. Among those that appeared in 2002 were *Briefing on Civil Rights Issues Facing Muslims and Arab Americans in Minnesota Post-September 11* (the commission also produced a similar study on Wisconsin); *Voting Rights in Florida 2002: Briefing Summary*; and *Haitian Asylum Seekers and U.S. Immigration Policy*.

#### ■ FURTHER READING:

##### ELECTRONIC:

Civil Rights Commission Approves Report Assailing Florida Vote. Cable News Network. <<http://www.cnn.com/2001/ALLPOLITICS/06/08/florida.vote/>> (January 29, 2003).

United States Commission on Civil Rights. <<http://www.usccr.gov>> (January 29, 2003).

## Communicable Diseases, Isolation, and Quarantine

■ BRENDA W. LERNER/K. LEE LERNER

Isolation and quarantine remain potent tools in the modern public health arsenal. Both procedures seek to control exposure to infected individuals or materials.

Isolation and quarantine are not synonymous. Isolation procedures are used with patients with a confirmed illness. Quarantine rules and procedures apply to individuals who are not currently ill—but who are known to have been exposed to the illness (e.g., the person has been in the company of a infected person or come in contact with infected materials).

Isolation and quarantine both act to restricts movement and slow or stop the spread of disease within a community. Depending on the illness, patients placed in isolation may be cared for in hospitals, specialized health care facilities, or in less severe cases, at home. Isolation is a standard procedure for active tuberculosis patients. In most cases, isolation is voluntary; however, isolation can be compelled by federal, state, and some local law.

Severe Acute Respiratory Syndrome (SARS) is the first emergent and easily transmissible disease to appear during the twenty-first century. Patients with SARS develop flu-like fever, headache, malaise, dry cough and other breathing difficulties. Many patients develop pneumonia and in 5% to 10% of cases, the pneumonia and other complications are severe enough to cause respiratory failure and death. SARS is caused by a virus that is transmitted mainly from person to person by the aerosolized droplets of virus.

SARS cases provided a test of recent reforms in international health regulations that were designed to increase surveillance and reporting of infectious disease—and to enhance cooperation in preventing the international spread of disease. Although not an act of bioterrorism, because the very same epidemiologic principles and isolation protocols might be used to both determine and initially respond to an act of bioterrorism, intelligence and public health officials closely monitored the political, scientific, and medical responses to the outbreak. In many regards, the SARS outbreak provided a real and deadly test of world public health responses, readiness, and resources.

Common to both the responses of the 2003 SARS outbreak and a potential deliberate biological attack using pathogens—including smallpox or anthrax—is the need to rapidly develop accurate diagnostic tests, treatment protocols, and medically sound control measures.

At the end of April, 2003, SARS had the potential to become a global pandemic. Scientists, public health authorities, and clinicians around the world struggled to both treat and investigate the disease.

The first known case of SARS was traced to a November, 2002, case in Guangdong province, China. By mid-February, 2003, Chinese health officials tracked more than 300 cases, including five deaths in Guangdong province from what was described at the time as an “acute respiratory syndrome.”

Many flu-causing viruses have previously originated from Guangdong Province because of cultural and exotic cuisine practices that bring animals, animal parts, and humans into close proximity. In such an environment, pathogens can more easily leap from animal hosts to humans. The first cases of SARS showed high rates among Guangdong food handlers and chefs.

Chinese health officials initially remained silent about the outbreak and no special precautions were taken to limit travel or prevent the spread of the disease. The world health community had no chance to institute testing, isolation, and quarantine measure that might have prevented the subsequent global spread of the disease.

On Feb. 21, Liu Jianlun, a 64-year-old Chinese physician from Zhongshan hospital (later determined to have unknowingly been a “super-spreader”—a highly contagious infected individual) traveled to Hong Kong despite the fact that he had a fever to attend a family wedding. Epidemiologists subsequently determined that Jianlun passed on the SARS virus to other guests at the Metropole Hotel where he stayed—including an American businessman en route to Hanoi, three women from Singapore, two Canadians, and a Hong Kong resident. Jianlun’s travel to Hong Kong and the subsequent travel of those he infected allowed SARS to spread from China to the infected traveler’s immediate destinations.

Johnny Chen, the American businessman, grew ill in Hanoi, Viet Nam, and was admitted to hospital. Chen infected 20 health care workers at the hospital including noted Italian epidemiologist Carlo Urbani who cared for him, and who worked at the Hanoi World Health Organization (WHO) office. Urbani first formally identified SARS as a unique disease on February 28, 2003. By early March, 22 hospital workers in Hanoi were ill with SARS.

Unaware of the emerging problems in China, the Urbani report drew increased attention among epidemiologists that in mid-March, Hong Kong health officials had also discovered an outbreak of an “acute respiratory syndrome” among health care workers. Unsuspecting hospital workers admitted the Hong Kong man infected by Jianlun to a general ward at the Prince of Wales Hospital because it was assumed he had a typical severe pneumonia—a fairly routine admission. The first notice that clinicians were dealing with an usual illness came—not from health notices from China of increasing illnesses and deaths due to SARS—but from the observation that that hospital staff, and those subsequently determined to have been in close proximity to the infected persons, began to show signs of illness. Eventually, 138 people, including 34 nurses, 20 doctors, 16 medical students, and 15 other health-care workers at the hospital contracted pneumonia.

One of the most intriguing aspects of the early Hong Kong cases was a cluster of more than 250 SARS cases that occurred in high-rise apartment buildings—many housing health care workers—that provided evidence of a high rate of secondary transmission. Epidemiologists conducted extensive investigations to rule out the hypothesis that the illnesses were related to some form of local contamination (e.g., sewage, bacteria on the ventilation system, etc.). Rumors started that illness was due to cockroaches or rodents, but no scientific evidence supported the hypothesis that the disease pathogen was carried by insects.

Hong Kong authorities then decided that those suffering from the flu-like symptoms would be given the option of self-isolation, with family members allowed to remain confined at home or in special camps. Compliance checks were conducted by police.

One of the Canadians infected in Hong Kong, Kwan Sui-Chu, returned to Toronto and died in a Toronto hospital on March 5. As in Hong Kong, because there were no alerts from China about the SARS outbreak, Canadian officials did suspect that Sui-Chu’s son and five health workers had been infected with a highly contagious virus. By mid April, Canada reported more than 130 SARS cases and 15 fatalities.

Increasingly faced with reports that provided evidence of global dissemination, on March 15, the World Health Organization (WHO) took the unusual step of issue a travel warning that described SARS is a “worldwide health threat.” WHO officials announced that SARS confirmed and potential cases had been tracked from China to Singapore, Thailand, Vietnam, Indonesia, Philippines, and Canada. Although the exact cause of the “acute respiratory syndrome” had not, at that time, been determined, the official issuance of the precautionary warning to travelers bound for South East Asia about the potential SARS risk severed notice to public health officials about the potential dangers of SARS.

Within days of the WHO warning, SARS cases were reported in United Kingdom, Spain, Slovenia, Germany, and in the United States.

WHO officials were initially encouraged that isolation procedures and alerts were working to stem the spread of SARS, because some countries reporting small numbers of cases experienced no further dissemination to hospital staff or others in contact with the SARS victims. However, in some countries, including Canada, where SARS cases occurred before WHO alerts, SARS continued to spread beyond the bounds of isolated patients.

WHO officials responded by recommending increased screening and quarantine measures that included mandatory screening of persons returning from visits to the most severely affected areas in China, Southeast Asia, and Hong Kong.

On March 29, Urbani, the scientist who first reported a SARS case, died of complications related to SARS.

In early April, WHO took the controversial additional step of recommending against “non-essential travel to

Hong Kong and the Guangdong province of China. The recommendation, sought by infectious disease specialists, was not controversial within the medical community, but caused immediate concern regarding the potentially widespread economic impacts.

World attention—focused largely on the ongoing war in Iraq—began to focus on SARS. Within China, under a new generation of political leadership, a politically unique event occurred when a Chinese official publicly apologized for a slow and inefficient response to the SARS outbreak. Allegations that officials covered up the true extent of the spread of the disease caused the dismissal of several local administrators including China's public health minister and the mayor of Beijing.

Mounting reports of SARS showed an increasing global dissemination of the virus. By April 9, the first confirmed reports of SARS cases in Africa reached WHO headquarters, and eight days later, a confirmed case was discovered in India.

Scientists scrambled to isolate, identify and sequence the pathogen responsible for SARS. Modes of transmission characteristic of viral transmission allowed scientists to place early attention on a group of viruses termed coronaviruses—some of which are associated the common cold. There was a global two-pronged attack on the SARS pathogen, with some efforts directed toward a positive identification and isolation of the virus, and other efforts directed toward discovering the genetic molecular structure and sequence of genes contained in the virus. The development of a genomic map of the precise nucleotide sequence in the virus would be key in any subsequent development of a definitive diagnostic test, the identification of effective anti-viral agents, and eventually a vaccine.

The development of a reliable and definitive diagnostic test was considered of paramount importance in keeping SARS from becoming a pandemic. A definitive diagnostic test would not only allow physicians earlier treatment options, but would also allow the earlier identification and isolation of potential carriers of the virus. Without advanced testing, physicians were forced to rely on less sensitive tests that were unable to identify SARS prior to 21 days of infection—in most cases too late to effectively isolate the patient.

In mid-April 2003, Canadian scientists at the British Columbia Cancer Agency in Vancouver announced that they had sequenced the genome of the coronavirus most likely to be the cause of SARS. Within days, scientists at the Centers for Disease Control offered a genomic map that confirmed more than 99% of the Canadian findings.

Both genetic maps were generated from studies of viruses isolated from SARS cases. The particular coronavirus mapped had a genomic sequence of 29,727 nucleotides—average for the family of coronavirus that typically contain between 29,000 to 31,000 nucleotides.

Proof that the coronavirus mapped was the specific virus responsible for SARS would eventually come from

animal testing, as rhesus monkeys were exposed to the virus via injection and inhalation, and then monitored to determine whether SARS like symptoms developed and if sick animals exhibited a histological pathology (i.e., an examination of the tissue and cellular level pathology) similar to findings in human patients. Other tests, including polymerase chain reaction (PCR) testing helped positively match the specific coronavirus present in the lung tissue, blood, and feces of infected animals to the exposure virus.

Identification of a specific pathogen can be a complex process, and positive identification requires thousands of tests. Testing is conducted with regard to testing Koch's postulates—the four conditions that must be met for an organism to be determined to be the cause of a disease. First, the organism must be present in every case of the disease. Second, the organism must be able to be isolated from the host and grown in laboratory conditions. Third, the disease must be reproduced when the isolated organism is introduced into another, healthy host. The fourth postulate stipulates that the same organism must be able to be recovered and purified from the host that was experimentally infected.

Early data indicate that SARS has an incubation period range of 2 to 10 days with an average incubation of about four days. This inoculation period allows the virus to be both transported and spread by an asymptomatic carrier. With air travel, asymptomatic carriers can travel to anywhere in the world. The initial symptoms are non-specific and common to the flu. Infected cases then typically spike a high fever (100.4°F) (38°C) as they develop a cough, shortness of breath, and difficulty breathing. SARS fulminates (reaches its maximum progression) in a severe pneumonia that can cause death.

As of May 1, 2003, no single therapy was demonstrated to show clinical effectiveness and physicians could offer only supportive therapy (e.g. administration of fluids, oxygen, ventilation, etc.).

Before the advent of vaccines and effective diagnostic tools, isolation and quarantine were the principal tools to control the spread of infectious disease. The term "quarantine" derives from the Italian *quarantena* and *quaranta giorni* and dates to the plague in Europe. As a precautionary measure, the government of Venice restricted entry into the port city and mandated that ships coming from areas of plague—or otherwise suspected of carrying plague—had to wait 40 days before being allowed to discharge their cargos.

The legal basis of quarantine in the United States was established in 1878 with the passage of Federal Quarantine Legislation in response to continued outbreaks of yellow fever, typhus, and cholera.

The public discussion of SARS related quarantine in the United States and Europe renewed tensions between the needs for public health precautions that safeguard society at large and the individual liberties. During the

later years of the nineteenth century and throughout the twentieth century, the law bent toward protecting the greater needs of protecting society. The fact that the poser of quarantine was sometime used to contain and discourage immigration, often made the use quarantine a political and well as medical issue. In other cases such, as with Tuberculosis (TB), quarantine proved effective and courts wielded wide authority to isolate, hospitalize, and force patients to take medications.

States governments within the United States have a general authority to set and enforce quarantine conditions. At the federal level, the CDC's Division of Global Migration and Quarantine, is empowered to detain, examine, or conditionally release (release with restrictions on movement or with a required treatment protocol) individuals suspected of carrying certain listed communicable diseases.

As of April 27, 2003, the Centers for Disease Control and Prevention (CDC) in Atlanta recommended SARS patients be voluntarily isolated, but had not recommended enforced isolation or quarantine. Regardless, CDC and other Public Health officials, including the Surgeon General, sought and secured increased powers to deal with SARS. On April 4, 2003, U.S. President George W. Bush signed Presidential Executive Order 13295 that added SARS to a list of quarantinable communicable diseases. The order provided health officials with the broader powers to seek "... apprehension, detention, or conditional release of individuals to prevent the introduction, transmission, or spread of suspected communicable diseases..."

Other diseases on the U.S. communicable disease list, specified pursuant to section 361(b) of the Public Health Service Act, include "Cholera; Diphtheria; infectious Tuberculosis; Plague; Smallpox; Yellow Fever; and Viral Hemorrhagic Fevers (Lassa, Marburg, Ebola, Crimean-Congo, and others not yet isolated or named)."

Canada, hit early and much harder by SARS than the U.S., responded by closing schools and some hospitals in impacted areas. Canadian health officials advised seemingly healthy travelers from areas with known SARS cases to enter into a 10-day voluntary quarantine. Once in isolation, individuals were asked to frequently take their temperature and remain separated from other family members. Within a month, almost 10,000 people were in some form of quarantine. Despite the mounting medical and scientific evidence, Canadian government officials, including the Prime Minister Jean Chrétien complained bitterly when, on April 23, the WHO recommended a postponement of non-essential travel to Toronto. Chrétien's government fearful that Canada's economy—already strained from tensions caused by the Chrétien—led government's failure to support the United States during the U.S. war against Iraq—might suffer further economic isolation.

Faced with a more immediate danger and larger numbers of initial cases, an authoritarian government in

Singapore was less hesitant in ordering quarantine of victims and those potentially exposed to the virus. One of the three Singapore women initially infected in Hong Kong turned out to be a super-spreader who infected more than 90 people. She recovered, but both her mother and father died of SARS.

Passengers arriving in Singapore coming from other countries with SARS are required to undergo questioning by nurses in isolation gear and then are required to walk through a thermal scanner calibrated to detect an elevated body temperature. Soldiers immediately escort those with elevated temperatures into quarantine facilities. Those subsequently allowed to remain in their homes are monitored by video cameras and electronic wristbands.

By late April 2003, WHO officials had confirmed reports of more than 3,000 cases of SARS from 18 different countries with 111 deaths attributed to the disease. Each new day brought new reports that increased these totals. United States health officials reported 193 cases with no deaths. Significantly, all but 20 of the U.S. cases were linked to travel to infected areas and the other 20 cases were accounted for by secondary transmission from infected patients to family members and health care workers.

In China, fear of a widespread outbreak in Beijing caused a late, but intensive effort to isolate SARS victims and halt the spread of the disease. By the end of April, 2003, schools in Beijing were closed as were many public areas were closed. Despite these measures, SARS cases and deaths continued to mount into late April. Many of China's neighbors considered closing borders to all but essential travel. Health authorities assert that the emergent virus responsible for SARS will remain endemic (part of the natural array of viruses) in many regions of China well after the current outbreak is resolved.

On April 28, 2003, the WHO declared that Vietnam was the first country to control its SARS outbreak, as no new cases were identified in 20 days (twice the usual incubation period). By August 2003, the initial outbreak was contained.

## ■ FURTHER READING:

### PERIODICALS:

Ksiazek, T. G., et al. "A Novel Coronavirus Associated with Severe Acute Respiratory Syndrome." *New England Journal of Medicine* 10.1056 (April 10, 2003): a030781.

Rosenthal, E. "From China's Provinces, a Crafty Germ Spreads." *New York Times*. (April 27, 2003).

### ELECTRONIC:

CDC. "Severe Acute Respiratory Syndrome (SARS)." April 3, 2003. <<http://www.cdc.gov/ncidod/sars/isolationquarantine.htm>> (April 27, 2003).

World Health Organization. Communicable Disease Surveillance & Response (CSR). April 24, 2003 <<http://www.who.int/csr/sars/en/>> (April 27, 2003).

SEE ALSO

*Biological Warfare, Advanced Diagnostics  
Biological Weapons, Genetic Identification  
Bioshield Project  
Bioterrorism  
Bioterrorism, Protective Measures  
CDC (United States Centers for Disease Control and  
Prevention)  
Public Health Service (PHS), United States*

## Communications System, United States National

■ JUDSON KNIGHT

The United States National Communications System (NCS) brings together representatives of numerous government departments, using a wide variety of technologies, to provide a single, integrated communications network in the interests of national security. Created in 1962, when Cold War tensions highlighted the need for reliable intra- and international communication, NCS underwent significant changes in 1984, but its core mission—to provide for the communication needs of the president and the national security apparatus—has not altered significantly.

**The “Red Telephone” and the reality of NCS.** One of the great fixtures of American national-security lore in the modern era is the “Red Telephone.” According to legend, this piece of equipment is exactly what its name implies: presumably an ordinary-looking phone colored a standard shade of red—but with a key difference. As it is depicted in movies and the popular imagination, the Red Telephone has no dial or buttons, because it is designed for communication between two sites only: the Oval Office and the Kremlin. In a moment of grave national danger, so the legend goes, the president of the United States picks up the Red Telephone and is instantly connected to his counterpart in Moscow.

The Red Telephone, in fact, is a figment of overactive imaginations. There is no Red Telephone, *per se*; rather, the president communicates with world leaders through various secure lines, which are maintained by NCS. The latter organization—and, perhaps, the myth of the Red Telephone itself—emerged from a period when the United States came as close as it ever would to nuclear war with the Soviet Union.

**Early history.** During the two weeks of the Cuban Missile Crisis in October 1962, as President John F. Kennedy spent a great deal of time communicating with Soviet General

Secretary Nikita Khrushchev, as well as with other world political and military leaders. Faulty communications technology threatened to further complicate interchanges, and thus exacerbate tensions, a situation that prompted Kennedy to action after the crisis subsided.

The president ordered a study of available security communication capabilities. Subsequently an interdepartmental committee, formed by the National Security Council (NSC), conducted this investigation. The committee recommended the creation of unified system designed to serve the security communication needs of the president and other top political, military, national security, and diplomatic figures. As a result, Kennedy established NCS by a presidential directive signed on August 21, 1963.

Its initial mandate called on NCS to link, improve, and extend the communications technology and capabilities of the relevant federal agencies and departments, with a focus on interconnectivity and the ability to survive ruptures in the communication system. It was a bold mission at a time when telephones had dials, few homes had more than one phone (let alone more than one phone line), and few offices possessed any equipment other than a phone and a typewriter. For the next two decades, the system continued on the model set for it in the early 1960s; then, on April 3, 1984, President Ronald Reagan greatly altered its structure with Executive Order (E.O.) 12472.

**NCS participants and NS/EP responsibilities.** Under the terms of E.O. 12472, NCS grew from six member agencies and departments to 22, and set about coordinating national security and emergency preparedness (NS/EP) plans to provide communications in the event of crisis or disaster. Today NCS works with all the departments of the federal government, as well as the Central Intelligence, National Security, and Federal Emergency Management agencies; the Joint Staff; the General Services, National Aeronautics and Space, and National Telecommunications and Information administrations; the Nuclear Regulatory and Federal Communications commissions; the Federal Reserve Board; and the United States Postal service.

A particularly notable example of a department with critical NS/EP responsibilities is the Department of Defense (DoD). Among the telecommunications assets it oversees are the Advanced Research Projects Agency (ARPA) computer network; the Direct Communications Link (the Washington-Moscow hotline that constitutes the real-life “Red Telephone”), the Defense Satellite Communications System; the Worldwide Military Command and Control System; and several others.

Along with the other 21 members, DoD is represented on NCS through the Committee for National Security and Emergency Preparedness. The committee, formerly known as the NCS Committee of Principals, was established by E.O. 12472, and renamed October 2001 according to E.O. 13231, “Critical Infrastructure Protection in the Information Age.” In late 2002, NCS was slated for inclusion in the new Department of Homeland Security.

## ■ FURTHER READING:

### BOOKS:

*National Communications System, 1963–1998: 35th Anniversary.* Arlington, VA: National Communications System, 1998.

*National Communications System for Emergency Response Personnel.* Washington, D.C.: Government Printing Office, 2001.

### PERIODICALS:

Caterinicchia, Dan. "When Duty Calls." *Federal Computer Week* 16, no. 36 (October 7, 2002): 25–26.

McConnell, Bruce. "Telecom Role Model." *Federal Computer Week* 16, no. 40 (November 11, 2002): 27.

### ELECTRONIC:

National Communication System. <<http://www.ncs.gov>> (January 29, 2003).

### SEE ALSO

*Cuban Missile Crisis*

*National Telecommunications Information Administration, and Security for the Radio Frequency Spectrum, United States*

*NSC (National Security Council)*

## Comprehensive Radiation Sensors (CRS).

SEE *Environmental Measurements Laboratory.*

# Comprehensive Test Ban Treaty (CTBT)

■ LARRY GILMAN

The Comprehensive Test Ban Treaty (CTBT) is an international agreement designed to end the testing of nuclear explosives. As of March, 2003, the United States is one of the 166 states that have signed the treaty, but the CTBT will only "enter into force" (i.e., take on the force of law for all ratifying states) when 44 "nuclear-capable" countries specifically listed in the treaty have all ratified the treaty. Of these 44 states, India, Pakistan, and North Korea have refused to sign, and 13 (including the U.S.) have signed but not ratified.

**Nuclear Testing.** Nuclear testing is the detonation of nuclear weapons for test purposes. Testing is needed to verify new bomb designs and to observe the effects of nuclear

weapons (e.g., types and amounts of radiation produced). The first nuclear test, codenamed Trinity, was conducted by the United States on July 16, 1945, near Alamogordo, New Mexico. Since that time, six other nations—China, France, India, Pakistan, the Soviet Union, and the United Kingdom—have conducted nuclear tests. (Some experts assert, based on U.S. intelligence satellite data, that Israel and South Africa may have conducted a joint nuclear test at sea in 1979.) The most recent nuclear test was conducted by India, on May 30, 1998.

Nuclear tests can be conducted underground, under water, in space, or in the atmosphere. No nuclear weapon has ever been tested in space, but approximately 2050 have been detonated in various environments on Earth. Before 1962, most tests were conducted in the atmosphere; the U.S. conducted 193 atmospheric tests between 1946 and 1962, and the Soviet Union conducted 142 such tests between 1948 and 1962. During the late 1950s and early 1960s, these atmospheric tests became a global political concern because of the radioactive substances they released into the air (fallout). The most problematic of these byproducts was iodine 131, a radioactive isotope of iodine. Iodine 131, which is chemically identical to ordinary iodine, can settle on grass, be consumed by cows, concentrate in milk, and further concentrate in the thyroid glands of human beings who drink the milk, especially children. Atmospheric testing in the 1950s and early 1960s released large quantities of iodine 131 into the atmosphere; in 1997, the U.S. National Cancer Institute estimated that 160 million people in the United States had been exposed to some level of iodine 131 from U.S. nuclear tests conducted in Nevada, and that these exposures would, over time, cause 30,000–75,000 cases of thyroid cancer. Although the extent of fallout exposure was not known at the time to be this large, public sentiment against testing became strong. As a result, the U.S., United Kingdom, and Soviet Union signed the Limited Test Ban Treaty on July 25, 1963. The Limited Test Ban Treaty forbade the detonation of nuclear weapons in the air, the sea, or space. The treaty went into effect on October 11, 1963; both superpowers conducted a flurry of atmospheric tests before the deadline, after which testing moved underground. The U.S. and Soviet Union had attempted to negotiate a "comprehensive" test ban treaty in 1963—that is, an agreement to ban *all* nuclear tests—but could not come to agreement on technical details. Also, military officials of both countries opposed a comprehensive test ban, wishing to continue developing new varieties of nuclear weapon. The Limited Test Ban Treaty committed its signatories to continuing to seek, in the words of the treaty's first article, "the discontinuance of all test explosions of nuclear weapons for all time"—in other words, a comprehensive test ban treaty.

The next legal step toward this goal occurred in 1974, when the Treaty on Underground Nuclear Weapons Tests (also known as the Threshold Test Ban Treaty) was signed by the U.S. and Soviet Union. This treaty forbade either



nation to conduct an underground test of any nuclear weapon with an explosive force greater than 150 kilotons (i.e., equivalent to that of 150,000 tons of TNT [trinitrotoluene]). The treaty has been observed by both parties since 1974, but did not enter into full legal force until December 11, 1990, when U.S. concerns about verification had been met. (Verification of a nuclear test ban treaty requires the collection of seismic and other data to assure that no test has been secretly performed that exceeds the limits of the agreement.)

In 1991, Soviet President Mikhail Gorbachev announced that the Soviet Union would unilaterally cease nuclear testing for one year. In 1992, a bill was passed by both houses of the U.S. Congress mandating a unilateral U.S. testing moratorium to respond to the Soviet testing halt. This bill was signed into law by President George H. Bush on October 2, 1992. Neither Russia (the nuclear inheritor-state of the Soviet Union) nor the U.S. have, as of early 2003, conducted any nuclear tests since the beginnings of these moratoria.

Multinational negotiations toward a CTBT began in Geneva, Switzerland on January 25, 1994. In June 1995, while CTBT negotiations were still under way, France announced that it would resume nuclear testing. This decision aroused official protest from many governments, including that of the United States, and a worldwide boycott of French-made goods. China, too, was continuing to perform sporadic nuclear tests during this period, and on June 20, 1996 India announced that it would not sign the CTBT. Nevertheless, on September 10, 1996, the CTBT was approved by a 158-to-3 vote of a special session of the United Nations General Assembly. President Clinton signed the CTBT for the U.S. on September 24, 1996, and was soon followed by representatives of many other states, including China, the United Kingdom, France, and Russia.

Since signing of the CTBT began in 1996, the only nuclear explosions to have taken place have been the nuclear tests by Pakistan and India in 1998, a total of 11 explosions.

**Ratification.** President Clinton's 1996 signature did not make the CTBT binding law for the U.S. U.S. commitment to such a treaty, like that of most other states, occurs in two steps: first "signature" (by a president or qualified ambassador), then "ratification" (formal agreement to the treaty by the legislative body of the state, e.g., Parliament or Congress). Many states obey the terms of treaties that they have signed but not yet ratified, while reserving to themselves the right to begin disregarding the provisions of the treaty at any time.

The U.S. signed the CTBT in 1996, but the Senate refused in 1999 to ratify (51 to 48). As of March 2003, United States president George W. Bush's administration has stated that it intends to continue observing the CTBT's ban on testing, but will not support ratification of the CTBT. Also, administration officials have indicated that

the U.S. may, at some time, withdraw from the treaty altogether. The Bush administration's Nuclear Posture Review of 2002, a document designed to guide nuclear-weapons strategy for years to come, has recommended that the U.S. develop a class of relatively low-yield nuclear weapons that would dive deep into the ground (probably at thousands of miles per hour) before exploding; the goal of such weapons, termed Robust Nuclear Earth Penetrators or "bunker busters," would be to destroy deeply buried targets. In order to develop such devices, the U.S. would have to resume testing of nuclear weapons.

**Verification.** Verification of the CTBT is accomplished by a global system of sensors termed the International Monitoring System (IMS). The IMS consists of sensors that detect bomb-type vibrations in the Earth, oceans, and air (termed seismic, hydroacoustic, and infrasonic vibrations, respectively) and that test the air for radioactive substances (radionuclides) which would reveal the occurrence of nuclear tests. The IMS is designed to accommodate 170 seismic monitoring stations, 11 hydroacoustic stations, 60 infrasound stations, and 80 radionuclide-detecting stations. These automatic sensors, deployed to provide global coverage, will report their data in real time via satellite to a monitoring center in Vienna, Austria, the International Data Centre (IDC). The IMS and IDC are run by an independent group, the Comprehensive Nuclear-Test-Ban Treaty Organization. (Since the CTBT is not officially "in force," the Comprehensive Nuclear-Test-Ban Treaty Organization has been funded by nonbinding international agreement.) Construction of the IMS began in 1997. Regardless of the legal future of the CTBT itself, the IMS will probably continue to provide high-quality, publicly-available information about nuclear testing worldwide.

#### ■ FURTHER READING:

##### BOOKS:

Galindo, Marta and John Newton. "Installation of New Stations in the Hydroacoustic Monitoring Network for the Comprehensive Test Ban Treaty," in proceedings from the *Oceans 2000 MTS/IEEE Conference and Exhibition*, IEEE, 797-801, 2000.

##### ELECTRONIC:

"The Comprehensive Nuclear Test-Ban Treaty." United States Department of State. January 10, 2001. <<http://www.state.gov/www/global/arms/treaties/ctb.html>> (March 10, 2003).

"The Limited Nuclear Test-Ban Treaty." United States Department of State. [No date on Web page.] <<http://www.state.gov/t/ac/trt/4797.htm>> (March 10, 2003).

##### SEE ALSO

*Antiballistic Missile Treaty*  
*Nuclear Weapons*  
*Start I Treaty*  
*START II*

## Computer and Electronic Data Destruction

Computers are often the repository of an astounding amount of information. Even in a stand-alone computer that is not linked to the Internet, millions of conventional pages of text and images can be stored in the hard drive and on peripherals, such as a floppy disk or on a compact disk (CD).

For sensitive operations, the security of computer data must be ensured. This is particularly true when data is erased. The convention version of data removal involves the deletion of a file, by the movement of the file to a “garbage can” (i.e., the “Recycling Bin” in the various Windows operating systems). This form of deletion instructs the computer to use the slice of hard or floppy disk space for something else. Eventually, the file will be overwritten. But, until that occurs, the information is recoverable.

The true cleaning of a hard or floppy disk involves overwriting the actual data. Computer data is recorded as a series of 0s and 1s. Irrevocable erasure of data can be achieved by rewriting the relevant sector of a drive with 0’s. Others advocate for a hexadecimal pattern (i.e., 110000001) followed by a “second pass”, which overwrites the hexadecimal pattern as 00111110. In this way, every unit of information has been changed at least once.

True cleaning of a CD is also possible. The data layer that was previously “burned” onto the CDs surface can be removed and ground into fine powder. The original polycarbonate disk that remains contains no trace of the original data. The CD, which is rendered unusable, can be conventionally disposed of.

Destruction can also be a brute force physical process. For example, a hard drive can be physically damaged so that it cannot be read, even if installed into another computer. Floppy disks can be cut apart. Thus, while information may still reside on the drive, that information is essentially destroyed. Disks and CDs can even be melted down.

A number of vendors offer data destruction services to those having concerns about the sensitivity and vulnerability of their data. Government agencies usually have in-house staff and facilities, so that sensitive information does not pass into unauthorized hands, even during the destruction process.

### ■ FURTHER READING:

#### BOOKS:

Bosworth, Seymour and Michael E. Kabay. *Computer Security Handbook*. New York: John Wiley & Sons, 2002.

Eoghan, Casey. *Digital Evidence and Computer Crime*. New York: Academic Press, 2000.

Kruse, Warren G., II., and Jay G. Heiser. *Computer Forensics: Incident Response Essentials*. Boston: Addison Wesley Professional, 2001.

#### SEE ALSO

*Computer Virus*

*Electronic Communication Intercepts, Legal Issues*  
*Information Security*

## Computer Fraud and Abuse Act of 1986

■ ADRIENNE WILMOTH LERNER

The United States Computer Fraud and Abuse Act of 1986 served to define criminal fraud and abuse for computer crimes on the federal level. The act specified a misdemeanor crime for the trafficking and misuse of passwords, and two felony offenses for unauthorized access to federal information systems and private computers deemed to have a “federal interest.” The act removed several legal ambiguities that surrounded computer information theft, such as the lack of specific legislation mentioning computers and the slightness of legal precedence in such cases.

Computer data systems of varying sorts had been used by the United States government since the 1960s. In the early 1980s, the first computers for business and home use were available in the marketplace. This expanse of the computer-owning and software-literate population forced the government to begin finding ways to protect data, either through encryption or protective barrier mechanisms around certain files. With the advent of intranets and computer-to-computer communication through telephone lines, hacking, or the breaking into other computer systems, became more commonplace. In 1981, a computer-savvy 24-year-old named Ian Murphy hacked into several government systems, including the White House switchboard. Murphy used the switchboard to order various products before turning his attention to cracking the codes protecting sensitive military files. Murphy was arrested, but prosecutors did not have the legal recourse to try him for computer crimes, as no such laws existed. Murphy was eventually convicted of theft and knowingly receiving stolen goods.

By 1982, Congress began collecting data on computer crime, and gathering testimony from computer fraud victims. Most of the victims were major corporations who did not want their security breaches and vulnerability to become public knowledge. Not only was it easy for random hackers to crack a system, but also corporations could hack into the data systems of rival companies, engaging in corporate espionage. After five years, Congress introduced the Computer Fraud and Abuse Act of 1986. The bill

passed decisively. That same session, the Electronic Communication Privacy Act of 1986 was passed, criminalizing the seizure and interception of digital messages and communication signals.

In January of 1989, Herbert Zinn was the first person to be convicted under the Computer Fraud and Abuse Act. As a teenager, Zinn broke into computer systems at the Department of Defense, wreaking havoc with several hundred files. Zinn was sentenced to nine months in prison and fined; he would have possibly received a harsher judgment if he had been over eighteen years-old at the time of the crime.

Since its inception, the Computer Fraud and Abuse Act has weathered changing technology and the development of the Internet. However, computer crime is once again on the rise, and only a fraction of victims report these crimes. Subsequent court proceedings and legislation such as the Compute Abuse Amendments Act of 1994 have provided specific wording criminalizing the promulgation of computer viruses and other damaging code.

#### SEE ALSO

*Computer Hackers*  
*Information Security*

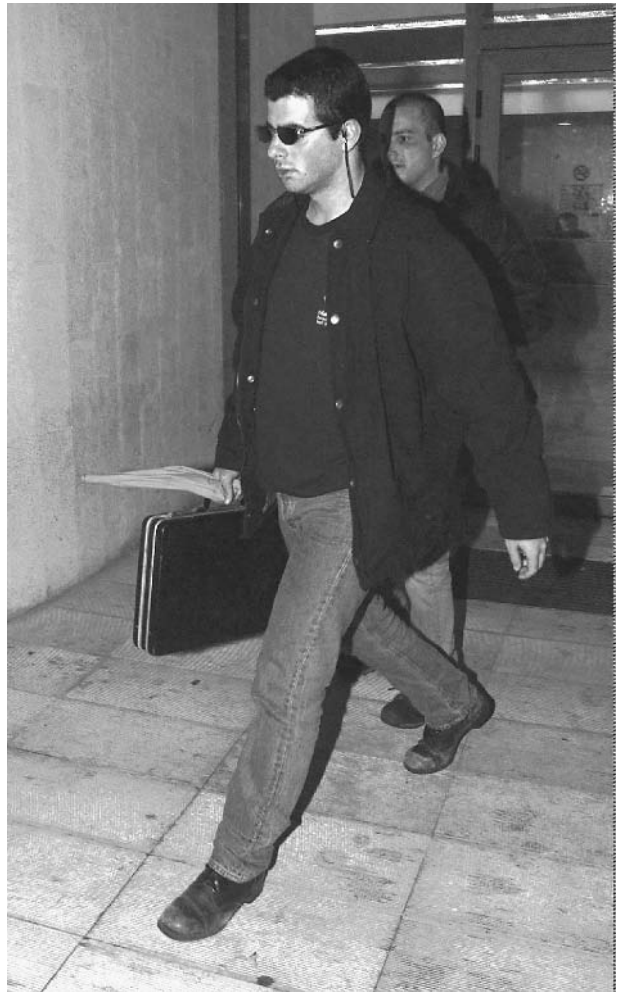
## Computer Hackers

Computer hackers are people who gain remote access (typically unauthorized and unapproved) to files stored in another computer, or even to the operating system of the computer. In the 1950 and 1960s, hackers were motivated more by a desire to learn the operating characteristics of a computer than by any malicious intent. Indeed, in those days hackers were often legitimate computer programmers who were seeking ways of routing information more quickly through the then-cumbersome operating system of computers.

Since then, however, computer hacking has become much more sophisticated, organized, and, in many cases, illegal. Some hackers are motivated by a desire to cripple sensitive sites, make mischief, and to acquire restricted information.

In the late 1990s, several computer hackers attempted to gain access to files in the computer network at the Pentagon. The incidents, which were dubbed Solar Sunrise, were regarded as a dress rehearsal for a later and more malicious cyber-attack, and stimulated a revamping of the military's computer defenses. In another example, computer hackers were able to gain access to patient files at the Indiana University School of Medicine in February 2003.

The threats to civilian privacy and national security from computer hackers was deemed so urgent that the



Ehud Tenebaum leaves a police station near Tel Aviv, Israel, under house arrest with two other Israeli teenagers in 1998 pending charges for the most organized hacker attack ever perpetrated on the Pentagon's computer system. AP/WIDE WORLD PHOTOS.

U.S. government enacted the Cyber-Security Enhancement Act in July 2002, as part of the Homeland Security measures in the wake of the terrorist attacks on September 11, 2001. Under this legislation, hackers can be regarded as terrorists, and can be imprisoned for up to 20 years.

One tool that a hacker can use to compromise an individual computer or a computer network is a virus. Depending on their design and intent, the consequences of a virus can range from the inconvenient (i.e., defacing of a Web site) to the catastrophic (i.e., disabling of a computer network). Within a few years during the 1990s, the number of known computer viruses increased to over 30,000. That number is now upwards of 100,000, with new viruses appearing virtually daily.

Despite the threat that they can pose, computer hackers can also be of benefit. By exposing the flaws in a computer network, hackers can aid in the redesign of the



Convicted computer hacker Kevin Mitnick, right, after being released from the Federal Correction Institute in Lompoc, California, in 2000, remained under a judge's order barring him from using a computer for a further three years. AP/WIDE WORLD PHOTOS.

system to make information more inaccessible to unauthorized access.

#### ■ FURTHER READING:

##### BOOKS:

McClure, Stuart, Joel Scambray, and George Kurtz. *Hacking Exposed: Network Security Secrets and Solutions*, 4th ed. Emeryville, CA: McGraw-Hill Osborne Media, 2003.

Spitzner, Lance. *Honeypots: Tracking Hackers*. Boston: Addison Wesley Professional, 2002.

Wang, Wallace. *Steal This Computer Book 3: What They Won't Tell You About the Internet*. San Francisco: No Starch Press, 2003.

Warren, Henry S., Jr. *Hacker's Delight*. Boston: Addison Wesley Professional, 2002.

##### SEE ALSO

*Computer Fraud and Abuse Act of 1986*  
*Cyber Security*  
*Internet Tracking and Tracing*

## Computer Hardware Security

■ BRIAN HOYLE

A phenomenal amount of information now resides on computers. Individual computers as well as computers that communicate with each other in geographically-restricted local networks as well as globally, via the Internet, contain billions of pages of text, graphics, and other sources of information. Without safeguards, this information is vulnerable to misuse or theft.

Computer security can take two forms. Software security provides barriers and other cyber-tools that protect programs, files, and the information flow to and from a computer. Hardware security protects the machine and peripheral hardware from theft and from electronic intrusion and damage.

Physical on-site security can be as easy as confining mission-critical computers to a locked room, and restricting access to only those who are authorized. This also holds for servers, which are computers that function as a central routing point for information to and from the

networked computers and the Internet. Many personal computer users pay to have this service provided by an Internet service provider (ISP). However, having an outside provider can generate security threats and can be disruptive if the ISP ceases operation. Nowadays, many corporations opt to establish an in-house ISP. In this way the security of the corporate server is under direct control.

Computers also have an internal form of a lock and key. A security password that is needed to gain access to all of a computer's functions can be stored on a chip known as the BIOS chip. Unfortunately, a dedicated thief can easily circumvent this hardware security feature, by removing the hard drive and putting it into another computer with a different BIOS chip.

With the exploding popularity of the Internet, hardware security has been extended to this electronic realm. Computers that are connected to the Internet are vulnerable to remote access, sabotage, and eavesdropping unless security measures are in place to buffer the computer from the outside electronic world.

Many corporations whose computers are linked to one another, employ a local version of the Internet. An Intranet or Local Area Network allows the exchange of information between the linked computers, while at the same time enabling the erection of hardware and software (i.e., firewalls) that screen information flowing to and from the Internet. Remote users of the internal network, such as telecommuting employees, can be protected through what is known as a virtual private network (VPN). A VPN establishes a protected communications link across a public network between the remote computer and the computers physically linked in the local network.

The individual computers that are linked in a network, and the dedicated devices that route information back and forth, are also known as nodes. The security measures that have been discussed above also function to safeguard nodes.

At the core of a network is a device called the hub. The hub exchanges the information between all of the connected computers. As such, it is key to a network. A hub should be kept away from high traffic areas, and preferably in a secure room. This restricts tampering.

While a hub relays information indiscriminately from computer to computer, a device called a switch is more selective. Information can be sent to one user computer but not to another. The use of a switch allows a network administrator to control the information flow to authorized viewers, which can be a security issue.

Fluctuations in the power supply can play havoc with computers. For example, a blackout or brownout can cause a computer to shut down abruptly. Information that is stored only in short-term memory will be lost. As well, the fluctuation can physically damage computer components. The use of a surge protector guards against electrical spikes and drops. An uninterruptible power supply (UPS) can also be hooked up to a computer. A UPS is essentially a battery that will power the computer in the

event of a power outage. This can provide time for information to be saved and for a computer to be shut down correctly.

#### ■ FURTHER READING :

##### BOOKS:

Bentley, Tom, and Jon Hastings. *Safe Computing: How to Protect Your Computer, Your Body, Your Data, Your Money and Your Privacy in the Information Age*. Concord, CA: Untechnical Press, 2000.

Bishop, Matt. *Computer Security: Art and Science*. Boston: Addison Wesley Professional, 2002.

Luber, Alan D. *PC Fear Factor: The Ultimate PC Disaster Prevention Guide*. Indianapolis: Que, 2002.

##### SEE ALSO

*Computer Keystroke Recorder*  
*Cyber Security*

---

## Computer Keystroke Recorder

---

A computer keystroke recorder, as its name suggests, is simply a device for sequentially recording all the keys pressed on a computer keyboard. Keystroke recorders are available commercially, but much more sophisticated devices are used by government agencies such as the Federal Bureau of Investigation (FBI).

Also called a keystroke logger, key logger, or keylogger, a computer keystroke recorder is a program that runs in the background as the computer operates, recording all key depressions or strokes. Some such devices are plugged in manually, but the more effective kind operate through means of a computer program. The latter may be introduced to the computer by means of a trojan horse, a remotely inserted program that operates much like a virus.

An example of an FBI keystroke-recording trojan is Magic Lantern, which made it possible to log keystrokes by means of a computer virus sent to a remote user's machine. The revelation of the device's use, reported by MSNBC News on December 12, 2001, invoked the ire of civil libertarians, as well as computer companies whose assistance the government sought. According to the MSNBC report, vendors of anti-virus software refused to cooperate with FBI requests to bypass special government-created trojans and viruses used for security purposes.

The FBI and its computer keystroke recording technology also made the news in late 2001 due to its involvement in *United States v. Scarfo*. The first known case of its kind, *Scarfo* involved a request by the defense to allow analysis of the keystroke recording technique used to gather evidence against the defendant. The government

claimed protection of classified information under the Classified Information Procedures Act (CIPA), and the court granted the government's motion.

#### ■ FURTHER READING:

##### PERIODICALS:

Hentoff, Nat. "The FBI's Magic Lantern." *Village Voice*. 47, no. 22 (June 4, 2002): p. 35.

Huleatt, Richard S. "EPIC May Never Learn Details of Government Keystroke Monitor." *Information Intelligence Online Newsletter* 22, no. 10 (October 2001): 5–6.

##### ELECTRONIC:

FBI Confirms "Magic Lantern" Exists. MSNBC. <<http://www.msnbc.com/news/671981.asp>> (January 27, 2003).

##### SEE ALSO

*Classified Information*  
*Computer Hardware Security*

---

## Computer Modeling

---

#### ■ JUDSON KNIGHT

Modeling, in the technical use of the term, refers to the translation of objects or phenomena from the real world into mathematical equations. Computer modeling is the representation of three-dimensional objects on a computer, using some form of software designed for the purpose. Among the uses of computer modeling are war games and disaster simulations, situations in which computers offer a safe, relatively inexpensive means of creating or re-creating events without the attendant loss of life or property.

### Mathematics, Computers, and Modeling Software

Mathematical modeling dates to advances in geometry and other disciplines during the late eighteenth century. Among these was the descriptive geometry of French mathematician Gaspard Monge, whose technique was so valuable to Napoleon's artillery that it remained a classified defense secret for many years. Nearly one and a half centuries later, at the end of World War II, mathematicians and scientists working for the United States war effort developed a machine for readily translating mathematical models into forms easily grasped by non-mathematicians.

That machine was the computer, and during the last two decades of the twentieth century, varieties of three-dimensional modeling software proliferated. These included any number of computer animation and gaming

packages, as well as varieties of computer-aided design/computer-aided manufacturing (CAD/CAM) systems. CAD allowed engineers and architects, for instance, to create elaborate models that allowed them to "see into" unbuilt structures, and to test the vulnerabilities of those structures without risking lives or dollars.

One notable variety of three-dimensional software is virtual reality modeling language, abbreviated VRML and pronounced "ver-mal." Necessary for representing three-dimensional objects on the World Wide Web (that portion of the Internet to which general users are most accustomed), VRML creates a virtual world, or hyperspace, that can be viewed through the two-dimensional computer screen. By pressing designated keys, the user is able to move not only up, down, right, and left, but forward and backward, within this virtual world.

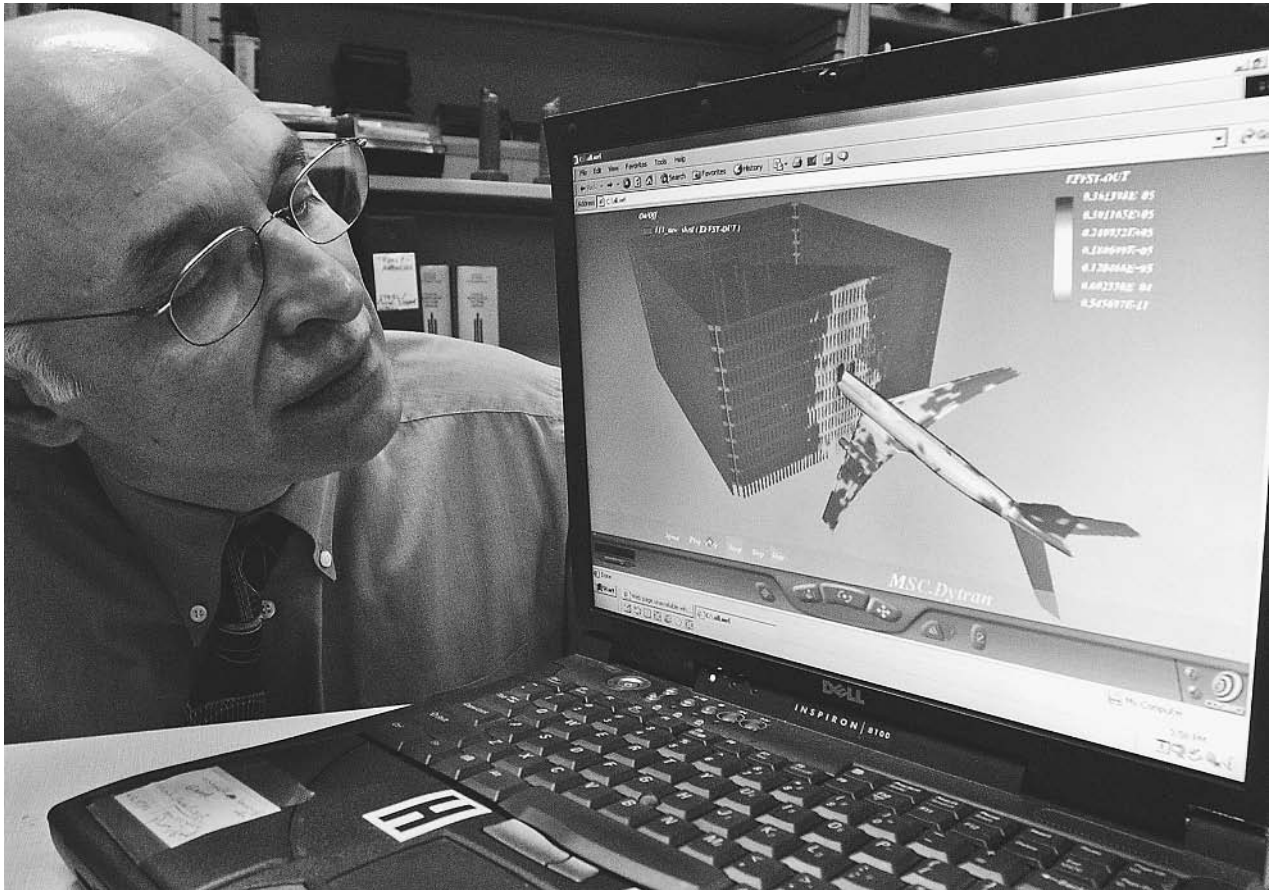
### Disasters, Wars, and Other Simulations

After the space shuttle *Columbia* crashed on February 1, 2003, analysts at the National Aeronautics and Space Administration (NASA) used modeling software applied by the National Transportation Safety Board (NTSB) for studying crashes. In applications such as those for the NASA and NTSB studies, the purpose is to understand not only what happened, but how and why it happened, and what caused it.

The more data available on a disaster, the better the model, and this in turn gives investigators more accurate tools for analysis. In the end, however, there is no substitute for human reasoning. For example, an NTSB simulation of the Swissair Flight 111 crash in September 1998 tracked the course of a fire from the cockpit that eventually brought down the plane, but it did not explain what caused the fire.

Still, the simulation is invaluable inasmuch as it provides human minds with an extraordinarily accurate and vivid source of information as to the exact sequence of events that took place during a disaster. NASA analysts used computer modeling to study the first great shuttle disaster, that of *Challenger* in 1986, but the technology of 2003 was vastly superior. Not only was a \$2,000 computer capable of running simulations that required a \$75,000 machine 17 years earlier, but advances in graphics—spurred, ironically, by the seemingly frivolous demands of gaming and the movies—had resulted in a vastly more accurate picture of what happened.

**War games and terror simulations.** The connection between entertainment and simulation in general, as well as computer modeling technology in particular, has not been lost on the U.S. security and defense leadership. In the immediate aftermath of the September 11, 2001, terrorist attack, federal officials brought together a team that included David Fincher, director of *Seven* and *Fight Club*; Steven E.



A steel structure expert at the University of California, Berkeley, studies a three-dimensional computer model of the airliner hitting the 96th floor of the World Trade Center. AP/WIDE WORLD PHOTOS.

De Souza, screenwriter for *Die Hard*; and Spike Jonze, director of *Being John Malkovich*. The assignment placed before these creative minds was one ideally suited to Hollywood: to imagine scenarios in which terrorists attacked the United States.

These scenarios, along with other forms of input, have helped form the basis for simulations by groups such as the Institute for Creative Technologies (ICT), a research center at the University of Southern California at Los Angeles. ICT is one of many entities in which the federal government invests nearly \$100 million a year for the purpose of developing military simulations—studies that, unlike the disaster models for NTSB or NASA, are concerned not so much with what has happened as with what *could* happen. The Department of Defense also has its own simulation think tanks, including the U.S. Army Simulation, Training, and Instrumentation Command, known as STRICOM.

Simulations developed by ICT are mind-boggling in their degree of verisimilitude. The “virtual humans” on screen are not automatons; rather, they have been programmed with personalities and emotions, like characters in a movie. Cutting-edge computer technology makes it

possible to even simulate smells. In an unusual merger of public and private sectors, ICT has sold commercial versions of games it co-produced with the U.S. Army.

The purpose of simulations produced by ICT and others involved in computer modeling goes far beyond mere entertainment: at a fraction of the expense and risk involved in war games involving real troops and equipment, commanders and their subordinates can study and learn from battle. Computer modeling also makes it possible to study dozens of different terror, but without any human or financial cost. By providing laboratories for instruction, simulations may prevent losses in real situations.

#### ■ FURTHER READING:

##### BOOKS:

- Danby, J. M. A. *Computer Modeling: From Sports to Spaceflight—From Order to Chaos*. Richmond, VA: Willmann-Bell, 1997.
- Emmer, Michele. *The Visual Mind: Art and Mathematics*. Cambridge, MA: MIT Press, 1993.

*Modeling and Simulation: Linking Entertainment and Defense.* Washington, D.C.: National Academy Press, 1997.

#### ELECTRONIC:

Lee, David B., Lt. Col., USAF. "War Gaming: Thinking for the Future." *Airpower Journal* <<http://www.airpower.maxwell.af.mil/airchronicles/apj/3sum90.html>> (March 14, 2003).

U.S. Air Force Wargaming Institute. <<http://www.cadre.maxwell.af.mil/wargame/main.htm>> (March 14, 2003).

U.S. Army Program Executive Office for Simulation, Training, and Instrumentation. <<http://www.stricom.army.mil/>> (March 14, 2003).

#### SEE ALSO

*Internet*  
*NASA (National Air and Space Administration)*  
*NTSB (National Transportation Safety Board)*  
*Supercomputers*

## Computer Security Act (1987)

The Computer Security Act of 1987 is the first major United States government effort to legislate protection and defense for unclassified information in government-related computer systems. The act mandates the National Bureau of Standards to develop and implement procedures that improve the security and privacy of sensitive material and creates a means for establishing minimum acceptable security practices.

The CSA arose out of congressional concerns about computer database vulnerability and executive branch over-zealousness on computer matters. While the Department of Defense argued that unclassified information could be pieced together to create a national security threat, President Ronald Reagan's 1984 National Security Decision Directive 145 set information safeguards at such a high level that private computer data companies loudly complained to legislators about federal scrutiny of their customers. Congress decided to assess the vulnerability of government computers, develop technical and management strategies against access to sensitive information, and establish mandatory training for employees in computer and communication security. The resulting CSA also designates the creation of a twelve-member advisory board that meets at least three times per year and reports to the Secretary of Commerce, the Office of Management and Budget, the National Security Council, and Congress.

While the CSA is designed to prevent the release of sensitive information, the law specifically forbids any federal agency to withhold information requested under the Freedom of Information Act (FOIA). It also does not authorize any agency to limit, restrict, or regulate the collection, disclosure, use, or sale of privately owned or public

domain information. Despite this provision journalists have encountered increasing difficulty obtaining FOIA access to federal material stored in computer databases. Librarians have also observed that the Department of Defense, Department of Energy, and NASA release fewer documents to the public than in the years prior to CSA.

In light of the George W. Bush administration's concern with secrecy as an element of national security, the CSA will likely continue to be used to limit public access to government information.

#### ■ FURTHER READING:

##### BOOKS:

Blyth, Andrew and Gerald L. Kovacich. *Information Assurance: Surviving in the Information Environment.* London: Springer, 2001.

Martin, Shannon E. *Bits, Bytes, and Big Brother: Federal Information Control in the Technological Age.* Westport, CT: Praeger, 1995.

#### SEE ALSO

*Bush Administration (2001–), United States National Security Policy*  
*Classified Information*  
*Commerce Department Intelligence and Security Responsibilities, United States*  
*Computer Fraud and Abuse Act of 1986*  
*Computer Hackers*  
*Computer Hardware Security*  
*DOD (United States Department of Defense)*  
*DOE (United States Department of Energy)*  
*FOIA (Freedom of Information Act)*  
*Information Security*  
*NSC (National Security Council)*  
*Reagan Administration (1981–1989), United States National Security Policy*

## Computer Software Security

#### ■ BRIAN HOYLE

Computer software security refers to the use of software to prevent damage to computer files, programs, and operating systems, as well as to monitor a personal computer (PC) or laptop for theft.

**Anti-virus software.** A recommended feature for any computer that is connected to the Internet is software that protects the computer from viruses. Like biological viruses, computer viruses need the machinery of another host, in this case a computer, to make new copies of themselves and infect another host computer. There are upwards of





Computer security researcher Steve Gibson is seen in his home office in Laguna Hills, California, in April, 2002. Two years prior, Gibson was testing intrusion-detection software when he suddenly found a program running on his computer that he had unknowingly installed. The hidden program secretly tagged along with another program and monitored his Internet habits. AP/WIDE WORLD PHOTOS.

100,000 known viruses, with new viruses being detected literally every day.

Viruses can enter computers via different routes. A common route is as an attachment to an email. When the email is opened the virus is triggered to disrupt whatever computer code it has been targeted towards. Viruses that target email addresses can distribute themselves to other computers very quickly. An infamous example is the “Love” virus, which infected millions of computers worldwide within hours of its release in May 2000.

There are a wide variety of anti-virus software programs available that will recognize, quarantine and destroy many of these viruses. Anti-virus programs need to be updated frequently (often accomplished automatically “on-line” with some vendors products) to keep pace with the appearance of new viruses.

**Theft.** Next to viruses, theft represents the biggest security issue for computer users. Various hardware options are designed to lessen the chance of theft. Anti-theft software is also available. There are several software programs that aim to lessen the usability, and so the appeal, of a stolen computer (particularly laptop computers). In one setup, a registered identifier number is beamed out when the stolen computer is hooked up to the Internet. Proprietary

software can detect and even track the location of the sending computer. Another strategy uses motion-sensing software that is adjusted to the motion patterns of the normal user. A different range of motions that are uncharacteristic of the principle user can trigger an audio alarm. As well, the computer is triggered to shut down and reboot. The user then needs to supply a complicated password to use the computer and even to read the scrambled files (see below) from the hard drive. This protection occurs even when the computer is shut off.

**Data encryption and ownership.** Encryption is the scrambling of the data so as to make the data undecipherable. Encryption programs can scramble the data that is resident in the computer as well as data sent to another computer via email. The message can be reassembled to the original format if the receiving computer has an encryption program installed.

With contracts being sent over the Internet, the ownership and legal status of such information has become an important issue. Digital signatures can be affixed to a document sent via the Internet to establish ownership, in the same way that a signature on a paper contract is legally binding. Countries including the United States have sanctioned the use of digital signatures.

**Authorization and intrusion.** Software programs allow a hierarchy of approvals to be established for access to data. In a company, for example, senior managers can be authorized to view and even manipulate data that more junior personnel do not have access to. Other programs act as guardians of the data, and detect any unauthorized or unusual actions on the computer (i.e., hacking).

Computers connected to the Internet are often equipped with software known as a firewall. The firewall functions to monitor incoming transmissions and to restrict those that are deemed suspicious. It is a controlled gateway that limits who and what can pass through. A number of vendors offer firewall programs. Like anti-virus software, these programs can and should be frequently updated, since those who seek to maliciously gain remote access to computers are constantly developing methods to thwart the firewall barrier.

#### ■ FURTHER READING:

##### BOOKS:

- Bentley, Tom, and Jon Hastings. *Safe Computing: How to Protect Your Computer, Your Body, Your Data, Your Money and Your Privacy in the Information Age*. Concord, CA: Untechnical Press, 2000.
- Bishop, Matt. *Computer Security: Art and Science*. Boston: Addison Wesley Professional, 2002.
- Cheswick, William R., Steven M. Bellovin, and Aviel D. Rubin. *Firewalls and Internet Security: Repelling the Wiley Attacker, Second Edition*. Boston: Addison Wesley Professional, 2003.
- Stoll, Clifford. *Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage*. New York: Simon and Schuster, 2000.
- Whittaker, James A., and Herbert Thompson. *How to Break Software Security: Art and Science*. Boston: Addison Wesley Professional, 2002.

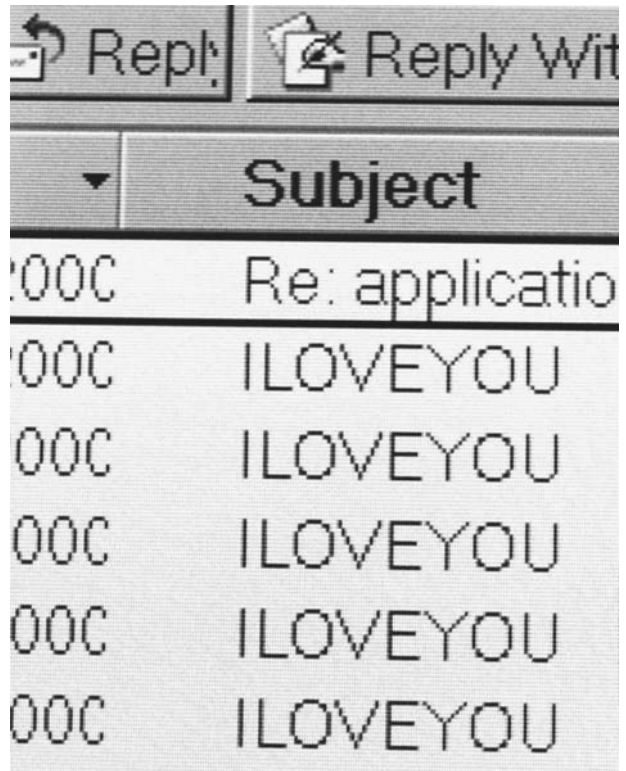
##### SEE ALSO

*Computer Hardware Security*  
*Computer Virus*  
*Cyber Security*

## Computer Virus

#### ■ LARRY GILMAN

A computer virus is a program or segment of executable computer code that is designed to reproduce itself in computer memory and, sometimes, to damage data. Viruses are generally short programs; they may either stand-alone or be embedded in larger bodies of code. The



A computer screen e-mail inbox showing subject names reading "ILOVEYOU," that contains a powerful computer virus that struck global communications systems and crippled government and corporate computer networks around the world in May, 2000. AP/WIDE WORLD PHOTOS.

term "virus" is applied to such code by analogy to biological viruses, microorganisms that force larger cells to manufacture new virus particles by inserting copies of their own genetic code into the larger cell's DNA. Because DNA can be viewed as a data-storage mechanism, the parallel between biological and computer viruses is remarkably exact.

Many viruses exploit computer networks to spread from computer to computer to computer, sending themselves either as e-mail messages over the Internet or directly over high-speed data links. Programs that spread copies of themselves over network connections of any kind are termed "worms," to distinguish them from programs that actively copy themselves only within the memory resources of a single computer. Some experts have sought to restrict the term "virus" to self-replicating code structures that embed themselves in larger programs and are executed only when a user runs the host program, and to restrict the term "worm" to stand-alone code that exploits network connections to spread (as opposed to, say, floppy disks or CD ROMs, which might spread a virus). However, virus terminology has shifted over the last decade, as computers that do not communicate over networks have become rare. So many worm/virus hybrids have appeared that any distinction between them is rapidly disappearing. In practice, any software that replicates itself may be termed a "virus," and most viruses are

designed to spread themselves over the Internet and are therefore “worms.”

A program that appears to perform a legitimate or harmless function, but is in fact designed to propagate a virus is often termed a Trojan Horse, after the hollow, apparently-harmless, giant wooden horse supposedly used by the ancient Greeks to sneak inside the walls of Troy and overthrow that city from within. Another interesting subclass of viruses consists of chain letters that purport to warn the recipient of a frightening computer virus currently attacking the world. The letter urges its recipient to make copies and send them to friends and colleagues. Such hoax letters do not contain executable code, but do exploit computerized communications and legitimate concern over real, executable-code viruses to achieve self-replication, spread fear, and waste time. Chain letters have also been used as carriers for executable viruses, which are attached to the chain letter as a supposedly entertaining or harmless program (e.g., one that will draw a Christmas card on the screen).

The first “wild” computer viruses, that is, viruses not designed as computer-science experiments but spreading through computers in the real world, appeared in the early 1980s and were designed to afflict Apple II personal computers. In 1984, the science fiction book *Necromancer*, by William Gibson, appeared; this book romanticized the hacking of giant corporate computers by brilliant freelance rebels, and is thought by some experts to have increased interest among young programmers in writing real-world viruses. The first IBM PC computer viruses appeared in 1986, and by 1988 virus infestations on a global scale had become a regular event. An anti-virus infrastructure began to appear at that time, and anti-virus experts have carried on a sort of running battle with virus writers ever since. As anti-virus software increases in sophistication, however, so do viruses, which thrive on loopholes in software of ever-increasing complexity. As recently as January 28, 2003, a virus dubbed “SQL Slammer” (SQL Server 2000, targeted by the virus, is a large software package run by many businesses and governments) made headlines by suspending or drastically slowing Internet service for millions of users worldwide. In the United States alone, some 13,000 automatic teller machines were shut down for most of a day.

All viruses cause some degree of harm by wasting resources, that is, filling a computer’s memory or, like SQL Slammer, clogging networks with copies of itself. These effects may cause data to be lost, but some viruses are designed specifically to delete files or issue a physically harmful series of instructions to hard drives. Such viruses are termed *destructive*. The number of destructive viruses has been rising for over a decade; in 1993 only about 10% of viruses were destructive, but by 2000 this number had risen to 35 percent.

Because even nonmalicious or nondestructive viruses may clog networks, shut down businesses or Web sites, and cause other computational harm (with possible real-world consequences, in some cases), both the private

sector and governments are increasingly dedicating resources to the prevention, detection, and defeat of viruses. Twenty to 30 new viruses are identified every day, and over 50,000 viruses have been detected and named since the early 1980s, when computers first became integrated with the world economy in large numbers. Most viruses are written merely as egotistical pranks, but a successful virus can cause serious losses. The ILOVEYOU virus that afflicted computers globally in May, 2000 is a dramatic recent case that illustrates many of the properties of viruses and worms.

The ILOVEYOU virus was so named because in its most common form (among some 14 variants) it spread by looking up address-book files on each computer it infected and sending an e-mail to all the addresses it found, including a copy of itself as an attachment named LOVE-LETTER-FOR-YOU.TXT.VBS. (“VBS” stands for Visual Basic Script, a type of file readable by World Wide Web browsers.) If a recipient of the e-mail opened the attachment, the ILOVEYOU virus code would run on their computer, raiding the recipient’s address book and sending out a fresh wave of e-mails to still other computers.

ILOVEYOU first appeared in Asia on May 4, 2000. Designed to run on PC-type desktop computers, it rapidly spread all over the world, infecting computers belonging to large corporations, media outlets, governments, banks, schools, and other groups. Many organizations were forced to take their networks off line, losing business or suspending services. The United States General Accounting Office later estimated that the losses inflicted by the ILOVEYOU virus may have totaled \$10 billion worldwide. Monetary losses occurred because of lost productivity, diversion of staff to virus containment, lost business opportunities, loss of data, and loss of consumer confidence (with subsequent loss of business).

National security may also be threatened by computer viruses and similar software objects. During the ILOVEYOU incident, the U.S. Department of Health and Human Services was disrupted for many hours. An official of the department stated that if a biological outbreak had occurred simultaneously with this ‘Love Bug’ infestation, the health and stability of the nation would have been compromised with the lack of computer network communication. An official at the U.S. Department of Defense stated that so many personnel had to be shifted from their primary responsibilities to deal with ILOVEYOU that if the incident had continued much longer, reservists would have had to be called up. All this damage, and more, was accomplished by a virus not even especially designed to do so. Governments are, therefore, concerned that specially designed viruses and other forms of cyberattack may be used deliberately by hostile governments or terrorist groups to cripple the military or the economy. The U.S. National Security Agency has stated that at least 100 governments are developing viruses and other cyberweapons, as well as terrorist groups. To counter such threats, the U.S. government has established a

National Infrastructure Protection Center in the Federal Bureau of Investigation. Its mission is to serve as the central federal point for coordinating information on threats to infrastructure, including threats (such as viruses) to computers and telecommunications networks.

#### ■ FURTHER READING:

##### BOOKS:

Ferbrache, David. *Pathology of Computer Viruses*. Germany: Springer-Verlag, 1992.

Fites, Philip, Peter Johnston, and Martin Kratz. *The Computer Virus Crisis*. New York: Van Nostrand Reinhold, 1992.

##### PERIODICALS:

"Virus Hits A.T.M.s and Computers Across Globe." *New York Times*. January 28, 2003.

##### ELECTRONIC:

Brock, Jack L. "'ILOVEYOU' Computer Virus Highlights Need for Improved Alert and Coordination Capabilities." United States General Accounting Office. Testimony before the Subcommittee on Financial Institutions, Committee on Banking, Housing and Urban Affairs, U.S. Senate. May 18, 2000. <nsi.org/library/virus/ai00181t.pdf> (Jan. 28, 2003).

##### SEE ALSO

*Cyber Security*

## Concealment Devices

#### ■ JUDSON KNIGHT

The need for concealment strikes at the heart of intelligence and covert operations work, as well as a number of military activities. Concealment devices have been used to disguise film, documents, and other items containing intelligence material, which of necessity must be transported from a dangerous location—in or around the spot where they were gathered—to a safe haven, namely the intelligence bureau that commissioned the activity. To achieve the objective of circumventing detection, intelligence agencies and operatives have developed a number of clever devices, ranging from hollow coins to fake batteries. Documents, cameras, and film had found secure hiding places in objects as innocuous as a statuette, a hairbrush, or a can of shaving cream.

### Camouflage and Concealment: Passive Arts

All forms of concealment devices rely on the use of camouflage in the most general sense of the term. The word,

from the French *camoufleur* ("to disguise"), entered the English language during World War I, when the development of military aircraft exposed troop positions to enemy reconnaissance planes. In the course of the war, all major military forces established camouflage units composed of soldiers trained in the art. This led to the development of camouflage uniforms, the use of foliage or other materials to disguise positions, and other measures.

Nature, of course, "discovered" camouflage long before humans did, and in a wide variety of plant and animal species, natural selection has favored those that developed protective coloration or other forms of natural camouflage. Concealment by camouflage, in its truest sense, is of necessity passive rather than active, and in this regard, the term does not encompass those species capable of imitating predators or otherwise "convincing" other plants or animals that they are something other than they are.

This point is an important one, because it is not the purpose of camouflage and concealment to persuade the enemy; rather, the purpose of camouflage is to render the enemy unaware. Disinformation, then, is not truly concealment, as its purpose is to convince the enemy that some (actually false) premise is the case. Likewise, codes and ciphers, while they certainly conceal information, are not a form of concealment in this sense because they are obviously codes.

### Varieties of Concealment Devices

Effective concealment necessarily involves items that resemble everyday objects, coins being a good example. During the Cold War, KGB operatives often carried microfilm in a concealment device made from one of the more physically large coins commonly used in the country of their operation. Likewise, a Western intelligence service in the late 1970s used a hollow version of a United States Eisenhower dollar coin.

Inside the Soviet version was a cavity for hiding microfilm, which might contain ciphers, messages, or a communiqué providing the operative with date and time coordinates for a planned transmission. A special pin opened the interior. The Western version, in use during the late 1970s, could be opened by pressing the tip of the eagle's wing on the reverse side.

Long before the use of coins as concealment devices, intelligence operatives utilized an even more common disk-shaped object of small size: a button. In this case, the button itself was an ordinary one, but the back contained a carefully written coded or enciphered message in very small lettering. This technique dates back to World War I.

**Hiding cameras.** A number of concealment devices, particularly those used by Soviet and East German intelligence, were designed to hide cameras inside ordinary-looking



Concealed weapons that fell into western hands through the defection of Russian Intelligence Captain Nikolai E. Khokhlov in 1954 included cases of cigarettes that fired hollowpoint bullets and miniature pistols that fired while making a sound less than the snap of a finger. AP/WIDE WORLD PHOTOS.

items. When West German operatives of the counterintelligence service BfV apprehended one East German spy, they found in his apartment a decorative wooden carving of an elk. Inside the base, however, was a compartment for holding a Minox camera, a favorite piece of photographic equipment on both sides of the iron curtain.

One reason for the Minox's popularity was its size and shape, which was oblong and flat, and therefore made for easy concealment. Another East German favorite was a men's clothing brush or shoe brush, which could easily hold a Minox in the handle. Locking pins kept the compartment from opening when the operative was using the brush for its intended purpose, as he would most certainly have done so as not to arouse suspicion.

A particularly inventive East German device made use of a portable chessboard whose surface had sockets to secure the playing pieces. One of the 64 sockets, when a paper clip was inserted into it, opened the back of the chessboard to reveal a microdot camera. The chessboard—which, like many of these items, was probably one of a

kind, created in a special East German workshop for espionage equipment. Security of intelligence operations required that no device become standard equipment; if one operative were detected, this could potentially blow the cover of other comrades using a similar item.

**Film and other items.** Cylindrical objects make a logical hiding place for rolls of film, and agencies of the Communist world used a number of such objects. One was a D-sized battery, about as large as a typical photographic film canister. So as to avoid suspicions arising from a non-working battery, inside the fake one was a much smaller battery, about the size of an AA, which provided voltage. This left the remainder of the inner compartment free to conceal any item small enough to fit.

For the same reason that the fake battery was made to work like a real one, a shaving-cream can device used by Western intelligence contained a small amount of shaving cream, with the remainder of the compartment set aside

for concealed items. A cigarette used by Polish intelligence likewise had real tobacco, but the operative would never knowingly light it: inside was a roll of extremely thin film. On the other hand, a soap case used by Czech intelligence to transport film did not have room for a real soap bar: inside was a battery and flashbulb, which would flash and ruin the film if it were opened improperly.

#### ■ FURTHER READING:

##### BOOKS:

Breckenridge, Robert P. *Modern Camouflage, the New Science of Protective Concealment*. New York: Farrar & Rinehart, 1942.

Hartcup, Guy. *Camouflage: A History of Concealment and Deception in War*. New York: Scribner's, 1980.

Minnery, John. *CIA Catalog of Clandestine Weapons, Tools, and Gadgets*. Boulder, CO: Paladin Press, 1990.

##### ELECTRONIC:

CIA Museum. Central Intelligence Agency. <<http://www.cia.gov/cia/information/artifacts/>> (March 29, 2003).

International Spy Museum. <<http://www.spymuseum.org/>> (March 29, 2003).

##### SEE ALSO

*Assassination Weapons, Mechanical Cameras*  
*Cameras, Miniature*  
*CIA Directorate of Science and Technology (DS&T)*  
*Covert Operations*  
*Cryptology, History*  
*Dead Drop Spike*  
*Disinformation*

## Consumer Product Safety Commission (CPSC), United States

The United States Consumer Product Safety Commission (CPSC) is an independent federal agency designed to protect the public against unreasonable risks of injuries and deaths associated with consumer products. Congress established the commission in 1972, as part of the Consumer Product Safety Act. The CPSC regulates more than 15,000 types of consumer products, from coffee pots to toys. The commission's jurisdiction, however, is limited. Cars, trucks, and motorcycles are governed by the U.S. Department of Transportation; the U.S. Food and Drug Administration (USFDA) oversees cosmetics, food and drugs. Alcohol, tobacco, and firearms fall under the domain of the U.S. Treasury Department.

Since its inception, the CPSC has conducted research on potential product hazards and vigorously pursued and enforced mandatory standards on many consumer products. The Consumer Product Safety Act requires manufacturers to report serious product defects in a timely manner. Failure to do so can result in civil penalties. In 2001, the commission fined Fisher-Price \$1.1 million on charges that it failed to disclose a fire hazard in a popular toy. The fine was the largest against a toy firm in CPSC's history.

Product recalls are one of the most familiar actions of the CPSC. Recall information is posted on the commission's Web site and circulated throughout the news media. One of the largest recalls in recent history involved 650,000 baby strollers that collapsed while in use. The CPSC and Ohio-based Century Products announced the historical recall after hundreds of children suffered injuries.

The backbone of the CPSC is the National Electronic Injury Surveillance System (NEISS). The system compiles data on consumer product-related injuries occurring in the U.S., as documented by hospital emergency departments. Such data allow the CPSC to make timely national estimates of the number of injuries associated with, although not necessarily caused by, specific consumer products. CPSC analysts study the data for important clues to the cause and potential prevention of injuries.

The Washington, D.C. headquartered agency has an operating budget of approximately \$56 million and employs approximately 480 people. In 2002, President George W. Bush nominated attorney Hal Stratton as the eighth chairman of the agency.

#### ■ FURTHER READING:

##### ELECTRONIC:

Consumer Product Safety Commission "Who We Are; What We Do For You." December 12, 2002 <<http://www.cpsc.gov/cpsc/pub/pubs/103.html>>(December 10, 2002).

##### SEE ALSO

*ATF (United States Bureau of Alcohol, Tobacco, and Firearms)*  
*FDA (United States Food and Drug Administration)*  
*NTSB (National Transportation Safety Board)*

## Continuity Irish Republican Army (CIRA)

Continuity Irish Republican Army (CIRA) also operates as, or is known as, the Continuity Army Council.



A consumer information officer with the U.S. Consumer Product Safety Commission demonstrates the danger crib slats can pose to an infant during a press conference in 2002. AP/WIDE WORLD PHOTOS.

CIRA is a radical terrorist splinter group formed in 1994 as the clandestine armed wing of Republican Sinn Fein (RSF), which split from Sinn Fein in the mid-1980s. "Continuity" refers to the group's belief that it is carrying on the original IRA goal of forcing the British out of Northern Ireland, and CIRA actively seeks to recruit IRA members. CIRA has been active in the border areas of Northern Ireland where it has carried out bombings, assassinations, kidnappings, extortion, and robberies. Targets include British military and Northern Ireland security targets and Northern Ireland Loyalist paramilitary groups. CIRA does not have an established presence on the U.K. mainland. As of May, 2002, CIRA was not observing an established cease-fire and in October, 2001, CIRA officials stated that decommissioning weapons would be "an act of treachery."

CIRA is estimated to have fewer than 50 dedicated activists, but is said to have recruited new members in Belfast. CIRA is suspected of receiving funds and arms from sympathizers in the United States. CIRA may have acquired arms and materiel from the Balkans in cooperation with the Real IRA.

#### ■ FURTHER READING:

##### ELECTRONIC:

CDI (Center for Defense Information), Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <<http://www.cdi.org/terrorism/terrorist.cfm>> (April 17, 2003).

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001," Annual Report: On the Record Briefing. May 21, 2002 <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual Reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

##### SEE ALSO

*Terrorism, Philosophical and Ideological Origins  
Terrorist and Para-State Organizations  
Terrorist Organization List, United States  
Terrorist Organizations, Freezing of Assets*

# Continuity of Government, United States

■ ADRIENNE WILMOTH LERNER

The Continuity of Government (COG) program ensures the survival of essential federal government leaders and agencies in the event of a severe crisis. Created at the height of 1960s public and government concern about the possibility of nuclear warfare, COG provides a network of disaster relief, emergency assistance, law enforcement, and information services to the general citizenry of the United States. COG also maintains underground facilities to protect the president, cabinet members, and essential government personnel in the event of attack or catastrophe.

President John F. Kennedy created the Continuity of Government program on February 12, 1962. The stated purpose of COG was to shield the essential infrastructure of the United States government from destruction, permitting its continued operation and authority in a time of crisis. Intended to preserve the American form of representative government, continuity of federal authority aided law enforcement, ensured general safety, and protected the government from the illegal assumption of power by rival foreign powers or anti-government organizations. The government acknowledged plans to construct secret facilities and implement a COG strategy, but the details and locations of COG operations were meant to remain secret.

The Kennedy administration incorporated existing emergency strategies into its COG plans. Executive Order 10346, issued by President Harry S. Truman in 1947, outlined emergency plans for federal departments. Truman created the Office of Emergency Planning to establish policies for continued operations in the event of a national crisis. Kennedy reorganized the Office of Emergency Planning as part of his wide-sweeping reform of national defense infrastructure. These reforms were dictated by Executive Order 10952, and the Office of Emergency Planning gained the authority to set policy for the continuity of all three main branches of government.

One of the first orders of the COG was to ensure the survival of the president, or executive authority. In 1947, the line of succession of to the presidency was expanded, and more firmly established. The line of succession moved first to the vice president, then to the Speaker of the House of Representatives, the president pro tem of the Senate, and then proceeds through nine members of the cabinet. Cabinet positions created after 1947 are not included in the line of presidential succession. COG used this established line of succession to determine its strategies for the preservation of executive function. According to COG policy, not all twelve people on the list of presidential

succession can gather in the same location, at the same time. During large, pan-government events, such as the State of the Union Address, and presidential inaugurations, one member of the Cabinet is removed to a remote, safe, COG-designated location.

After securing the line of succession in the Executive branch, the COG program mandated that individual government departments create their own, internal lines of succession and continuity plans. COG officials check these lines and plans annually, and most are published in the Federal Register, so that other agencies can coordinate operations with continuity personnel.

One of the most clandestine operations of the COG program is the maintenance of the so-called Shadow Cabinet. The Shadow Cabinet is composed of trained personnel, appointed by the president and cabinet to serve as a reserve government in the unlikely event of a catastrophic disaster that destroys the government in Washington. The Shadow Cabinet operates at a secure COG location, and has never been utilized or played any role in Federal policy formation.

COG plans also included the physical protection of government entities. The preeminent COG safe facility was constructed in stages, beginning in the 1940s. An extensive series of underground bunkers that contain all of the necessities of a small city, was constructed in the mountains of Virginia. The facility, known as Mount Weather, is one of a series of regional Crisis Relocation Facilities. Command centers for the Federal Emergency Management Agency (FEMA) and the National Emergency Coordinating Center are located deep within the cavernous structure. Other facilities designated as COG safe sites include several military bases and *Air Force One*, the president's personal airplane.

In the 1980s, the White House National Program Office was responsible for COG operations. Operations were expanded to include the establishment of facilities responsible for the maintenance of critical information systems, including government and banking computer systems. Emergency management agencies decided to house reserve command centers at Mount Weather, providing a central, underground, and contained location for COG operations.

As the Cold War ended, and details of the government's COG operations garnered public attention, debate emerged over the usefulness and possible effectiveness of COG plans. Critics alleged that the system was outdated; others claimed it was insufficient to handle a crisis of great magnitude. As the frenzy about nuclear weapons ebbed, the COG strategy was evaluated to handle post-cold war threats, such as terrorist attacks. Indeed, some aspects of the COG plan went into effect during the September 11, 2001, terrorist attacks on New York and Washington, D.C.

The recent creation of the Department of Homeland Security (DHS) will possibly alter current, established COG



plans. The DHS gained the authority to administer COG plans, and assumed responsibility for many of its member agencies. To compliment the federal COG program, DHS officials encouraged state and local governments to implement or reform their own COG strategies. New guidelines and annual audits will aid in the supervision of state and local COG plans, making sure that such plans provide an adequate guarantee of local law enforcement and government operation in the event of a crisis.

■ FURTHER READING:

ELECTRONIC:

Federal Emergency Management Agency. Mount Weather Emergency Assistance Center homepage. <<http://www.fema.gov/pte/weather.htm>> (20 April 2003).

SEE ALSO

*Emergency Response Teams*  
*FEMA (United States Federal Emergency Management Agency)*

other formulations, such drugs routinely carry warnings against operating heavy equipment under the influence of the drug. The impairment of judgment associated with dexamphetamine pills, further stimulates CAP research.

During the Flight of Apollo 13, as the crew entered the critical reentry orbit interface, the exhausted crew was reportedly ordered to take Dexedrine tablets to help keep their computer inputs precise and accurate.

Use of dexamphetamine by U.S. pilots, whose judgment might have been impaired by fatigue or the use of "go pills," was also argued to be a contributing factor in a 2002 "friendly fire" bombing accident in Afghanistan.

■ FURTHER READING:

ELECTRONIC:

DARPA, Defense Science Office. Continuous Assisted Performance (CAP). <<http://www.darpa.mil/dso/thrust/biosci/cap.htm>> (April 14, 2003).

SEE ALSO

*Information Warfare*  
*Interrogation: Torture Techniques and Technologies*

---

## Continuous Assisted Performance (CAP)

---

In order to extend the physical capabilities of soldiers and the mental acuity of pilots and other operators of technical equipment, the Defense Advanced Research Projects Agency (DARPA) sponsors research into continuous assisted performance (CAP) technology and pharmacology.

CAP programs are designed to allow an increase in operation tempo by allowing soldiers to operate without sleep, or limited amounts of sleep, for at least seven days. In most combat operational systems, the fatigue of soldiers is the major limiting factor in operational readiness and ability to continue action. Because of the increasingly technical nature of warfare, the mere ability to go without sleep is not productive unless high levels of both cognitive and physical performance can be maintained.

The effects of sleep deprivation are well known to interrogators, and informal efforts to fight fatigue among troops have ranged from the soldier's historical use of strong coffee or tea to the condoned use of pharmacological fatigue management tools. U.S. Air Force pilots are routinely allowed to take dexamphetamine pills (also known as "go" pills), a prescription drug.

The use of go pills is controversial because the active ingredients can impair judgment. In fact, when used in

---

## Coordinator for Counterterrorism, United States Office

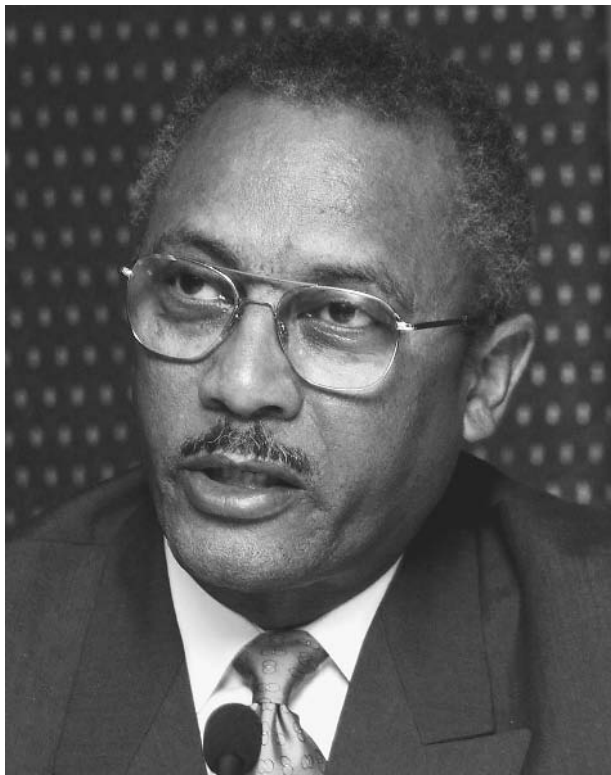
---

The Office of the Coordinator for Counterterrorism is a section of the United States Department of State charged with coordinating efforts to improve cooperation between the U.S. government and its foreign counterparts in battling terrorism. The coordinator, an ambassador, is the primary functionary of the federal government for developing and implementing America's counterterrorism policy.

### Four Principles of U.S. Counterterrorism Policy

In forming specific policies for tactical purposes, the coordinator considers four strategic principles of U.S. counterterrorism policy:

1. The government makes no concessions to, or agreements with, terrorists;
2. Terrorists must be brought to justice for their crimes;



U.S. State Department Coordinator for Counterterrorism, Francis X. Taylor, answers questions at a news conference in New Delhi, India, during a 2001 meeting to finalize a U.S./India anti-terrorism project. AP/WIDE WORLD PHOTOS.

3. States that sponsor terrorists and terrorism must be isolated and pressured so as to force a change of behavior; and

4. The counterterrorism capabilities of countries allied with the United States, and those that require assistance in fighting terrorism, must be bolstered.

Under provisions of the U.S. Patriot Act of 2001 (8 U.S.C. 1182), Section 411, the secretary of state may, in consultation with the attorney general of the United States, designate certain terrorist organizations on a "terrorist exclusion list" (TEL). Organizations listed on the TEL may be prevented from entering the country, and in certain circumstances may be deported. Before the secretary of state places an organization on the TEL, he or she must find that its members commit or incite terrorist activity, gather information on potential targets for terrorist activity, or provide material support to further terrorist activity. Under the terms of the statute, "terrorist activity" means all unlawful activity that involves hijacking or sabotage of an aircraft, vessel, or vehicle; hostage-taking; a violent attack on a person protected under international law; assassination; or the use of firearms, biological or chemical agents, nuclear devices, or other weapons to endanger individuals or damage property for purposes other than mere personal gain.

On December 5, 2001, Secretary of State Colin Powell, in consultation with Attorney General John Ashcroft, placed more than three dozen groups on the TEL. These represented a range of ideologies and areas of operation, including the Libyan Islamic Fighting Group, the Army for the Liberation of Rwanda, the Continuing Irish Republican Army, and the Japanese Red Army. Included also were front organizations such as the al-Hamati Sweets Bakeries, a Yemeni company considered to have ties with the Islamist terror organization al-Qaeda.

#### ■ FURTHER READING:

##### PERIODICALS:

Nelson, Scott Bernard. "U.S. Offers \$5M in Financial War on Terrorism." *Boston Globe*. (November 14, 2002): C1.

##### ELECTRONIC:

Coordinator for Counterterrorism. United States Department of State. <<http://www.state.gov/s/ct/>> (February 22, 2003).

##### SEE ALSO

*Department of State, United States FEST (United States Foreign Emergency Support Team) Terrorist Organization List, United States United States, Counter-Terrorism Policy*

---

## Copyright Security

---

The term *copyright security* refers to the protection of, and measures taken to prevent the unauthorized duplication of, copyrighted materials. With the increasing digitization and computerization of society, efforts aimed at maintaining and protecting copyright security have likewise become increasingly high-tech. Software is routinely copyright-protected, and copyright holders often take extraordinary measures, including the retention of detective agencies, to police acts of copyright infringement.

**Copyright law.** Article I, Section 8, of the United States Constitution authorizes Congress to protect the writings of authors, and to this end, Congress passed the U.S. Copyright Act (17 USC 101–810), the principal set of statutes governing copyright in America. Because the law is written to be interpreted broadly, and because it contains provisions precluding any state laws inconsistent with it, copyright law is almost entirely a federal and not a state matter.

In order to be protected by copyright, a work must be original, and must be in a concrete medium—in other



A steam roller crushes pirated CDs and electronic games during a destruction ceremony at the customs office in Bangkok, Thailand. AP/WIDE WORLD PHOTOS.

words, it must be recorded, not existing solely in “live” form. A work need not carry a copyright notice to be copyrighted, nor is registration required. However, copyright holders wishing to obtain registration may do so through the federal agency charged with administering copyright, the Copyright Office of the Library of Congress in Washington, D.C.

The holder of a copyright has the exclusive right to reproduce, distribute, perform, display, or license his or her work, as well as derivatives of his or her work. This means that others, in order to use all or a portion of that work, must obtain permission and, if necessary, pay a fee for use. There are, however, limited exceptions for “fair use” of copyrighted works, as in a book review.

Works published before 1923 are now in the public domain, meaning that they no longer hold a copyright, though a particular translation, made more recently, may be copyrighted. For works published after 1923, there are specific provisions as to when the item becomes part of the public domain. Some of these provisions, and other

aspects of U.S. copyright law, are governed by the Berne Convention for the Protection of Literary and Artistic Works, which the United States signed in 1989.

**The Digital Millennium Copyright Act.** As technology has changed, so has the definition of “writings” under U.S. copyright law. Today the Copyright Act encompasses not only those forms of expression traditionally understood as writings, but also architectural designs, works of graphic art, motion pictures, sound recordings, and computer software. Continued changes in the technology of copyrighted material prompted the 1998 passage of the Digital Millennium Copyright Act (DMCA), the most comprehensive overhaul of copyright law in a generation.

The DMCA endures criticism from detractors who consider it as squelching the free exchange of ideas through the Internet and electronic media. Although controversial, the DMCA remains law, and as such requires enforcement. Although federal authorities have sole power where enforcement is concerned, private firms such as BayTSP, a digital detective service, assist the federal government by interdicting lawbreakers. In addition to law enforcement agencies, Bay TSP’s clientele includes private holders of intellectual property who pay the company to protect that property against infringements in cyberspace.

Using an Internet spider (a computer program that crawls over the World Wide Web and automatically fetches Web pages, for instance for a search engine), BayTSP searches the Web for lawbreakers. These include, for its federal clients, purveyors of child pornography, and for its private clients, users offering electronic files to share. These electronic files may include software, sound recordings in digital format, or other materials.

If BayTSP finds an IP or Internet Protocol address (equivalent to a neighborhood post office on the Internet) at which illegal activity is taking place, under the DMCA, it has the right to subpoena logs kept by the Internet service provider. These logs will enable it to connect IP addresses with user accounts. Arrest of lawbreakers may follow, depending on the seriousness of the crime and the degree of desire for enforcement on the part of the client. For companies interested in maintaining good public relations, that desire may be low, whereas for federal agencies investigating child pornography, enforcement is usually swift and severe.

#### ■ FURTHER READING :

##### ELECTRONIC:

Cringley, Robert. “We Can Run, But We Can’t Hide: How BayTSP Is Enforcing the Digital Millennium.” Public Broadcasting System. <<http://www.pbs.org/cringely/pulpit/pulpit20020919.html>> (February 22, 2003).

Forno, Richard. Copyright, Security, and the Hollywood Hacking Bill. <<http://online.securityfocus.com/columnists/99>> (February 22, 2003).

## SEE ALSO

*Computer Software Security*

## Counterfeit Currency, Technology and the Manufacture

In the past, counterfeiters produced false banknotes with printing presses, and some of the more skillful counterfeiters went to great lengths to imitate the original. Today, sophisticated computer printers and copiers enable even unskilled would-be counterfeiters to produce notes that bear at least a superficial resemblance to real ones. However, the federal government continually works to stay a step or more ahead of counterfeiters, updating currency and making it ever more difficult to duplicate.

### Two Waves of Counterfeiting

For virtually as long as there has been regular currency, there has also been false currency, which has provided a highly lucrative illegal trade to those who can successfully pass off false banknotes as the genuine article. The period since the middle of the twentieth century has seen two significant waves of counterfeiting. First, there was a surge in the illegal production of banknotes during the 1960s, when advances in printing and graphic arts technology enabled counterfeiters with the right equipment and skills to produce highly accurate copies of federal currency. By the 1990s, however, counterfeiting by means of the printing press had diminished in significance compared to a new variety of counterfeit currency manufacture, this one using computer printers.

The phenomenon of “P-notes,” or “printer notes,” first came to the attention of law enforcement in the early 1990s. In 1995, authorities made a total of 37 arrests nationwide in connection with the production and distribution of currency produced on ink-jet or laser-jet printers. By 2000, this number had skyrocketed to 4,500 arrests, and officials estimated that P-notes accounted for as much as forty percent of the currency seized by the United States Secret Service (USSS) and other agencies annually.

**Contrast of practitioners and techniques.** The change in choice of technology also signaled a change in the profile of the average counterfeiter. The old variety of criminal operating in this field tended to be mature and skilled—a



A computer printout of counterfeit \$20 bills removed from the home of a Massachusetts teenager by the U. S. Secret Service. AP/WIDE WORLD PHOTOS.

professional, highly trained practitioner who usually possessed, or at least had access to, printing equipment whose operation would require knowledge far beyond that of a novice.

The 1990s variety of counterfeiter, by contrast, fit a quite different profile. Rather than being “professional counterfeiters,” they were more likely to be drug dealers who used their P-notes in connection with other crimes, most notably the purchase of drugs. Typically youthful (many were juveniles), these new counterfeiters lacked skills for counterfeiting. Whereas the old model at least required some degree of human ingenuity, the new type of counterfeiting was primarily a matter of possessing the right equipment.

Equipment loomed large in the old counterfeiting technology as well, but practitioners had to know how to use it. Counterfeiters of that era carefully studied currency, and made numerous photographs of it with graphic-arts cameras using different filters so as to break down the various stages of the printing process. Only after considerable trial and error could a workable set of printing plates be produced.

In contrast to this painstaking process, the new counterfeiting process required only that one use a high-quality scanner to obtain an image of a bill, then print that bill on a printer with high resolution. Given the ease of production, counterfeiting again became a growth industry during the

1990s, and in 2001, the federal government seized a record \$47 million in counterfeit currency. By the following year, the figure had dropped to \$43 million.

## Anti-counterfeiting Technology

The fact that the value of counterfeit currency seized in 2002 had dropped by almost 10 percent is not an indication of looser standards in interdiction; rather, after the September 11, 2001, terrorist attacks on the United States, the federal government was more likely to be aggressive in searching for counterfeiters, whose ranks could presumably include foreign operatives funding illegal operations while undermining the value of U.S. currency. The reduction in seizures is probably an indication of success in efforts by the federal government to make its currency more difficult to duplicate.

In 1996, partly as a response to the proliferation of P-bills, the U.S. currency underwent its first major redesign in 70 years. Already difficult to duplicate, the currency became much more so thanks to measures such as the use of optically variable ink (OVI). The latter contains tiny particles of special film such that it changes color depending on the angle from which it is viewed. Extremely expensive and therefore used in limited quantities, OVI is just one of several specialized varieties of ink used in producing currency. By 2004, additional changes included the introduction of new colors of inks. None is commercially available—another hurdle in the production of false currency.

A number of other features distinguish genuine currency from counterfeit. One of the most obvious ones is the paper itself. Every variety of national currency is made with a special type of paper (the Australian dollar is actually printed on very thin plastic), and U.S. currency uses a highly durable variety made from cotton pulp. Not only does it have a distinctive texture, it is far more resistant to tearing, deformation, moisture, or sunlight than most varieties of paper. Again, currency paper is not commercially available.

For the counterfeiter, a genuine banknote is a veritable minefield of potential pitfalls, and literally every square millimeter presents its own challenges. There are watermarks, embedded threads, see-through features, microprinting, holograms, latent images—even forms of embossing to facilitate recognition of various denominations by the blind and visually impaired. The printing of currency is also highly complicated, involving various processes at different stages. In addition to lithography, letterpress, and sometimes silkscreening, there is intaglio, an extremely expensive, technically difficult process in which the surface of the paper is deformed ever so slightly—another distinctive feature of official currency production.

**Special safeguards against copiers.** Aside from these challenges to the would-be counterfeiter, there is also the

problem of producing a usable serial number. Given these challenges, a drug dealer with a computer printer or copier is unlikely to enjoy long-term success in this illicit trade. For those using a copier, the problem is rendered even greater by additional measures. Most modern forms of currency have anti-copy features, tiny designs that have words such as *VOID* or *FAKE* embedded in them in such a way that they will be visible if copied.

Manufacturers of color copy machines have also implemented a number of measures to circumvent the use of their equipment for illegal purposes. Most modern copy machines carry and embed unique codes, invisible in ordinary light, such that their products are traceable to a specific machine. There is also technology that detects specific design elements of currency, and will cause the copier to shut down if it is used for illegal purposes.

### ■ FURTHER READING:

#### BOOKS:

- Optical Document Security.* Boston: Artech House, 1998.
- Sincerbox, Glenn T. *Counterfeit Deterrent Features for the Next-Generation Currency Design.* Washington, D.C.: National Academy Press, 1993.
- U.S. Currency: Treasury's Plan to Study Genuine and Counterfeit U.S. Currency Abroad: Report to Congressional Requesters.* Washington, D.C.: General Accounting Office, 1997.

#### ELECTRONIC:

- "Counterfeit Detection: A Guide to Spotting Counterfeit Currency." <<http://www.indigoimage.com/>> (February 5, 2003).
- "Technology Breeds New Counterfeiting." ABC News <[http://abcnews.go.com/sections/Downtown/2020/Downtown\\_010601\\_counterfeitmoney\\_feature.html](http://abcnews.go.com/sections/Downtown/2020/Downtown_010601_counterfeitmoney_feature.html)> (February 5, 2003).

#### SEE ALSO

- Engraving and Printing, United States Bureau Federal Reserve System, United States Secret Service, United States*

---

## Counter-Intelligence

---

Counter-intelligence is the use of intelligence resources to identify, circumvent, and neutralize the intelligence activities of a foreign power. That foreign power may be an enemy nation or a putative ally. In the United States, counter-intelligence is overseen from the Counter-intelligence Center (CIC) of the Central Intelligence Agency



Counter-intelligence agents are sworn in before a joint congressional committee holding open hearings on events surrounding the September 11, 2001 terrorist attacks. Behind the screen at lower left, used to protect their identities, are CIA and FBI agents. ©REUTERS NEWMEDIA INC./CORBIS.

(CIA), although a number of intelligence and law enforcement agencies are concerned with counter-intelligence to some degree.

Not only has the United States faced spying by Soviet and Eastern Bloc, Chinese, and Cuban operatives, but also by semi-friendly nations such as France or Indonesia, and by outright allies such as South Korea and Israel. According to testimony given before the House Permanent Select Committee in 2000 by Paul Redmond, former CIA associate deputy director of operations for counter-intelligence, some 41 countries were at that time attempting to spy on the United States. Given the size of the threat posed by foreign intelligence—which seeks to gain information on the technology and activities of the U.S. government, its agencies, and the military—federal authorities have sought to keep in place an effective counter-intelligence network. This involves not only operators, or front-line personnel involved in direct contact with foreign intelligence agents, but also analysts, whose job it is to study wiretap transcripts, surveillance reports, and other materials on the activities of foreign agents.

While the CIA holds the principal role in counter-intelligence among U.S. agencies, even the Federal Bureau of Investigation (FBI), whose primary responsibility is law enforcement, has a counter-intelligence role. Sometimes this can be inadvertent; FBI agents, rather than their counterparts in the CIA, apprehended Soviet operative John Walker in 1985. Actual FBI counter-intelligence is

concerned with investigating terrorist threats and other attempts to disrupt infrastructure or operations in the United States. (Ironically, an FBI counter-intelligence agent, Robert Hanssen, was exposed in 2001 as a spy of long standing for the Soviets and later Russia.)

Counter-intelligence may involve the employment of double agents, the planting of false information, or other efforts to undermine the intelligence-gathering activities of foreign nations. The agency conducting counter-intelligence may, when it has detected and identified foreign intelligence operatives, elect to keep those persons in place and not expose or arrest them—at least not for a time—in order to cause further detriment to the opposing intelligence agency by passing disinformation to the operative. This is a particularly likely option if the foreign agency represents a hostile power, rather than a friendly nation.

#### ■ FURTHER READING:

- Davis, James Kirkpatrick. *Spying on America: The FBI's Domestic Counter-intelligence Program*. New York: Praeger, 1992.
- Godson, Roy. *Dirty Tricks or Trump Cards: U.S. Covert Action and Counter-intelligence*. Washington, D.C.: Brassey's, 1995.
- Olson, James M. "The Ten Commandments of Counter-intelligence." *Studies in Intelligence* no. 11 (fall-winter 2001).

Parrish, Michael. *The Lesser Terror: Soviet State Security, 1939–1953*. Westport, CT: Praeger, 1996.

Richelson, Jeffrey T. *The U.S. Intelligence Community*, third edition. Boulder, CO: Westview Press, 1995.

SEE ALSO

*Domestic Intelligence*  
*Intelligence and Counterespionage Careers*

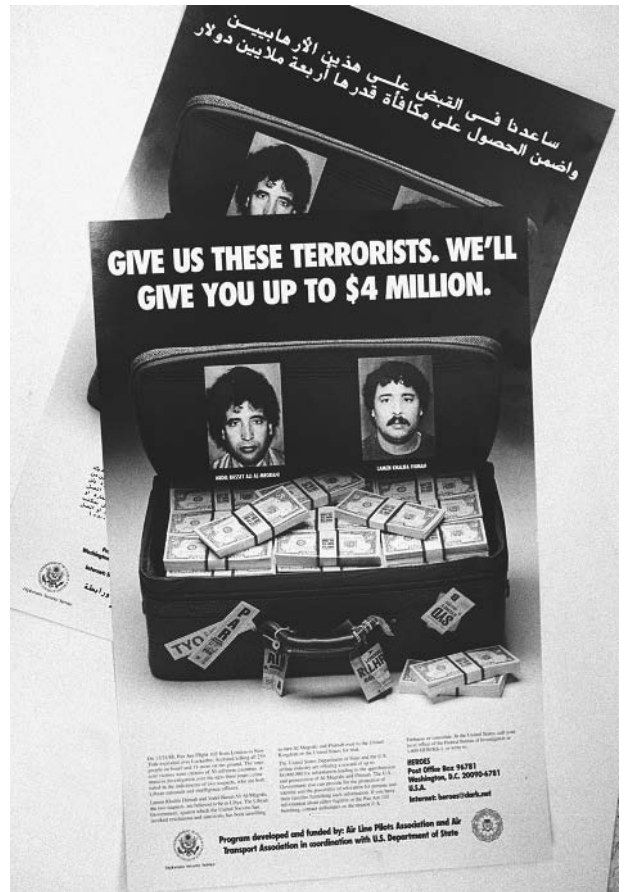
## Counter-Terrorism Rewards Program

The Counter-Terrorism Rewards Program, administered by the United States Department of State offers monetary compensation for individuals who volunteer information that leads to the location, capture, and trial of suspected terrorists. The program also seeks information relevant to finances, assets, and plans of terrorist organizations. The Federal Bureau of Investigation (FBI), and the Central Intelligence Agency (CIA) work closely with the Department of State to investigate all information garnered through the Counter-Terrorism Rewards Program. In 1998, after the bombing of United States embassies in East Africa, the Department of State raised the maximum reward for information to \$5 million.

The rewards program not only offers monetary rewards for information aiding anti-terrorism operations, but also promises confidentiality and anonymity for the informant. The United States government further promises to aid and relocate informants whose disclosure of information places themselves, and their family, in jeopardy.

The Counter-Terrorism Rewards Program is now a part of a larger anti-terrorism operation, the Rewards for Justice Program. The program pays for information relevant to the arrest and capture of wanted terrorists, both domestic and foreign. As part of the Patriot Act of 2001, the secretary of state can pay rewards greater than \$5 million for information leading to the arrest of suspected terrorists. To date, the program has paid \$9.75 million to 24 individuals who aided government anti-terror investigations.

The Counter-Terrorism Rewards Program, as part of Rewards for Justice, has had several key successes. Information received through the program led to the arrest and eventual conviction of the 1993 World Trade Center bomber, Ramzi Yousef. The highest current priority of the rewards program is information leading to the capture of al-Qaeda front man, Usama bin Laden, and others with suspected involvement in the 2001 attacks on the World Trade Center and the Pentagon.



Wanted posters, released in English and Arabic in 1995 by the FBI and State Department, show two suspects wanted in the bombing of Pan AM flight 103 which exploded over Lockerbie, Scotland in 1988. AP/WIDE WORLD PHOTOS.

■ FURTHER READING:

ELECTRONIC:

U.S. Department of State. "Rewards for Justice" (April, 29, 2003) <<http://www.rewardsforjustice.net/>>.

SEE ALSO

*Counter-Intelligence*  
*Homeland Security, United States Department*  
*September 11 Terrorist Attacks on the United States*



## Covert Operations

Covert operations are activities carried out by an intelligence or security agency, usually in a foreign country, in such a way that it is difficult to connect that agency with its action. Laws requiring free access to government information and an assertive press have provided Americans

# FRONT

The front of the leaflet features two black and white portraits. On the left is Aiman al-Zawahiri, wearing glasses and a white turban. On the right is Usama bin Laden, with a full beard and a white turban. Between the portraits, the text reads "UP TO \$25,000,000 REWARD". The names "AIMAN AL-ZAWAHIRI" and "USAMA BIN LADEN" are printed below their respective portraits. A small "AP/WIDE" logo is visible in the bottom right corner of the leaflet.

# BACK

PUSHTO	 USAMA BIN LADEN	DARI
UP TO A \$25,000,000 REWARD FOR INFORMATION LEADING TO THE WHEREABOUTS OR CAPTURE OF THESE TWO MEN.	 AIMAN AL-ZAWAHIRI	UP TO A \$25,000,000 REWARD FOR INFORMATION LEADING TO THE WHEREABOUTS OR CAPTURE OF THESE TWO MEN.

Leaflets dropped over Afghanistan by the U.S. military advertising rewards of up to \$25 million offered by the U.S. government for information leading to the capture of Usama bin Laden or his lieutenant Aiman al-Zawahiri. AP/WIDE WORLD PHOTOS.





Two members of a U.S.-led covert operations team stand in front of a downtown store in Kandahar, Afghanistan in March, 2002. AP/WIDE WORLD PHOTOS.

with much knowledge about their country's participation in covert operations, particularly during the Cold War. Some scholars have interpreted this information about covert operations as evidence of an aggressive American hand played in foreign policy, while others regard the United States as the most effective nation to bear the burden of world security and political stability.

## The Purpose of Covert Operations

For reasons that will be discussed below, most examinations of covert operations focus almost exclusively on U.S. covert operations, undertaken most prominently by the Central Intelligence Agency (CIA). Virtually every populated region has been the target of U.S. covert operations during the postwar era. This is particularly true of places in which the ruling regime is neither unreservedly hostile, nor unequivocally friendly, to the United States. Even a hostile regime that has failed to fully consolidate its power, such as Cuba in the period 1959–61 and Iran exactly 20 years later, may provide a promising area for covert operations.

Areas of focus in covert operations include the following: support, training and indoctrination, manipulation (including "dirty tricks"), and other covert activities. Support includes political advice to friendly parties, intelligence-gathering operations, monetary disbursements to individuals working in the service of U.S. interests, financial and technical help for pro-American political parties, and assistance to other private organizations such as labor unions and companies whose interests align with those of the United States.

Training and indoctrination areas of activity may include the dissemination of propaganda, which often must be covert in order to be effective. (An example from the late 1970s is the proliferation of editorial pieces in western European dailies that favorably compared the U.S. neutron bomb with the Soviet SS-20.) Also under this heading is the training of individuals, groups, and forces in a variety of techniques and areas of expertise.

Covert manipulation activities include economic operations, which can be designed either to destabilize the economy of a hostile power—in which case the action would qualify as a "dirty trick"—or to bolster the economy

of a friendly, but unstable nation. In the same way, paramilitary or political-action groups can be used to destabilize or overthrow a regime (a “dirty trick”), or they can help to support a pro-American government.

## A Brief History of U.S. Covert Operations

During the immediate post World War II years, the focus of covert operations was Europe—primarily in the East, but also in western nations such as France or Italy, where Communists threatened to take power, and where covert operations focused on supporting anti-Communist labor unions and parties. In the East, the focus was on destabilizing Soviet-backed regimes. CIA also backed hundreds of propaganda assets, most notably Radio Free Europe, Radio Liberty, Voice of America, and Radio Free Asia, which broadcast from the Philippines to Communist China.

During the 1950s and 1960s, attention shifted to the newly emergent Third World, including Cuba, the Dominican Republic, and several nations in Central America, where Communists either tried to gain control of governments (or, in the case of Cuba, succeeded); the Congo in Africa, where the rise of Patrice Lumumba threatened to destabilize the region; and several areas in southwest Asia, most notably Iran, whose Prime Minister Mohammed Mossadegh had nationalized the Anglo-Iranian Oil Company.

**The Carter years.** The CIA and other organizations undertook extensive covert operations during the war in Vietnam, but the late 1970s saw a sharp decline in these activities. A number of reasons influenced this change, not least among them the exposure of questionable CIA deeds that took place during the Church Committee hearings in the U.S. Senate. It could be argued that the hearings themselves were but one aspect of a larger and generalized distrust of government power that emerged in the aftermath of the 1960s, Vietnam, and Watergate.

In addition, the administration of President James Earl Carter publicly favored openness in government, and reductions in American adventurism overseas. Even so, during this time, the CIA still undertook or supported, covert operations in such arenas as Angola, South Yemen, and Afghanistan, but there was unquestionably a greater emphasis on propaganda as opposed to direct action during the Carter years.

**Reagan and Bush years.** During the 1960s and 1970s, Communists had either won control, were attempting to win control, or enjoyed the support of dozens of nations in Africa, Asia, and Latin America. At the same time, the

overthrow of the Shah in Iran portended the rise of another anti-American force, that of Islamic fundamentalism. Such were the challenges facing the administration of President Ronald Reagan when it took power in 1981.

Reagan responded to this situation by undertaking an array of covert operations unparalleled by that of any preceding administration. Reagan stepped up covert operations and support of anti-Communist forces in Afghanistan and Angola, as well as those in El Salvador. He sought to destabilize the Vietnamese-backed Communist regime in Cambodia, as well as the Communist Sandinistas in Nicaragua. Although Reagan was particularly active in the Middle East against Iraq, Libya, and Iran, the most notorious covert operation of the Reagan years involved collusion between the CIA and the Iranian government in an arms deal that would free U.S. hostages and fund the anti-Sandinista Contras.

Although the Iran-Contra scandal served to hamstring many of Reagan’s more ambitious undertakings, his covert operations did not end after the scandal broke in 1987. In 1989, successor George H. W. Bush conducted military operations against Panama’s dictator, General Manuel Noriega, who was captured and imprisoned. In this action, as in the Gulf War of 1991, the actual firing of shots followed a long period of covert operations.

As with Carter, the last Democrat in the White House, President William J. Clinton pledged openness, and presented his as an administration that was above the practice of covert operations. This was a relatively easy claim to make, since the end of the Cold War obviated many of Reagan’s and Bush’s undertakings. Furthermore, like the Church Committee hearings, the Iran-Contra affair served to bring the operations of the intelligence establishment under public scrutiny. Clinton’s administration, however, was one characterized by virtually unprecedented military adventurism, under a variety of guises: humanitarian support in Somalia, nation-building in Haiti, and countering an aggressive, genocidal force in Bosnia and Yugoslavia. In each case, military action would have been much more difficult and costly without covert operations providing advance intelligence.

Eight months into his administration, President George W. Bush declared war on terrorism soon after the terrorist attacks of September 11, 2001. The twentieth century was over, and with it both the Cold War and the post-Cold War era. The war on terror began with the bombing of Afghanistan on October 7, 2001, but by then, the CIA and other organizations had long since paved the way with extensive covert operations on the ground.

### ■ FURTHER READING:

#### BOOKS:

Borosage, Robert, and John D. Marks. *The CIA File*. New York: Grossman, 1976.

Knott, Stephen F. *Secret and Sanctioned: Covert Operations and the American Presidency*. New York: Oxford University Press, 1996.

Marshall, Jonathan, Peter Dale Scott, and Jane Haapiseva-Hunter. *The Iran-Contra Connection: Secret Teams and Covert Operations in the Reagan Era*. Boston: South End Press, 1987.

Prados, John. *President's Secret Wars: CIA and Pentagon Covert Operations since World War II*. New York: William Morrow, 1986.

Richelson, Jeffrey T. *The U.S. Intelligence Community*, third edition. Boulder, CO: Westview Press, 1995.

#### SEE ALSO

*Bay of Pigs*  
*Church Committee*  
*CIA (United States Central Intelligence Agency)*  
*Vietnam War*

## CPNB (Chemical and Biological National Security Program).

SEE *NNSA (United States National Nuclear Security Administration)*.

message. This would have been so no matter how carefully it had been enciphered or encoded, but the Germans sometimes made things even easier by sending the same message in plain text.

#### ■ FURTHER READING:

##### BOOKS:

Kahn, David. *Kahn on Codes: Secrets of the New Cryptology*. New York: Macmillan, 1983.

Konheim, Alan G. *Cryptography: A Primer*. New York: Wiley, 1981.

Lubbe, J. C. A. van der. *Basic Methods of Cryptography*. New York: Cambridge University Press, 1998.

Newton, David E. *Encyclopedia of Cryptology*. Santa Barbara, CA: ABC-CLIO, 1997.

#### SEE ALSO

*ADFGX Cipher*  
*Cryptology, History*

---

## Crime Prevention, Intelligence Agencies

---



---

### Crib

---

A crib is a section of an encoded or enciphered message that can easily be rendered into plain text, thus providing a tool whereby a skilled cryptanalyst can crack the entire code or message. A famous example of a “crib” from outside the world of espionage is the Rosetta Stone, used to translate Egyptian hieroglyphics.

Essentially a thank-you note from a group of priests to a magnanimous king, the stone was addressed to the second-century B.C. ruler Ptolemy V, who, like all the Ptolemies, spoke Greek rather than Egyptian. Therefore, the priests sent the note in Greek, as well as in hieroglyphics and demotic, a simplified version of hieroglyphic writing. Thus the French archaeologist Jean-François Champollion, who studied the Rosetta Stone in the early nineteenth century, was able to translate the Greek portion, and from this crack the code first of demotic, and then of hieroglyphics.

Any time a force sends out a message whose content is predictable to the enemy, this offers an opportunity for a resourceful cryptanalyst to find a crib. Thus, when the German high command in World War II sent greetings to Adolf Hitler every April 20—the Fuhrer’s birthday—it was fairly easy for Allied cryptanalysts to guess the gist of the

The relationship between law enforcement agencies such as the Federal Bureau of Investigation (FBI) and intelligence is straightforwardly recognized, as exemplified by the fact that the FBI is regularly involved in intelligence and counterintelligence activities. Less obvious, however, is the interaction between operations such as the Central Intelligence Agency (CIA) and crime prevention or law enforcement. Although most activities of intelligence organizations are by definition secret, it is at least possible to discern the outlines of a positive correlation between intelligence and crime prevention activities. In the case of police states and terrorist organizations, the relationship between intelligence and crime prevention—or, for covert operations in enemy countries, intelligence and the promotion of crime—is even easier to demonstrate.

**Totalitarian societies and radical movements.** One of the means to appreciate the interaction between intelligence and/or covert operations on the one hand, and crime prevention on the other, is to observe the example of totalitarian nations and the radical movements associated with them. In nations such as those of the Soviet bloc before the end of the Cold War, the presence of an intelligence-gathering entity such as the KGB was so pervasive that it had the side effect of virtually minimizing ordinary crime. While in the last two decades of the Soviet era, the

black market became an increasingly significant facet of daily life. In the centralized command economy that prevailed at that time, it was by definition a criminal enterprise to engage in the buying and selling of goods through channels other than those overseen by state authorities. Yet, as the Soviet economy declined, the black market became virtually the only means whereby individuals could obtain basic goods, let alone luxury items. This was true even of party apparatchiks other than the highest officials, and for this reason, the black market became the beneficiary of benign neglect on the part of Soviet authorities.

With the exception of the forms of commerce encompassed by the black market, however—and most such commerce would not be deemed criminal in a liberal democracy—the Soviet Union and its Eastern European satellites seem to have had a much lower crime rate than the United States and Western Europe over a comparable period. The obvious explanation for this difference, particularly when European countries are compared to make up for cultural differences, is the existence of a pervasive information-gathering apparatus. With spies, cameras, bugs, and tape recorders pervasive throughout society, criminal activity was unlikely to flourish unless it enjoyed official sanction.

**Promoting crime in liberal democracies.** Opposite to this obvious relationship between totalitarian societies, intelligence, and crime prevention is that between totalitarian or radical movements, intelligence, and the promotion of crime in liberal democracies. The founder of the Soviet state, V. I. Lenin, is credited as saying that “The enemy will sell us the rope with which we will hang him.” Lenin’s statement may have been too modest: based on the apparent relationship between the Soviet Union, allied movements and nations, and illegal activity in the West during the 1970s and 1980s, it appears in some cases that, to paraphrase Lenin, the enemy actually paid for the rope himself.

Although rumors of CIA involvement in the drug trade have long been fodder for conspiracy theories of various ideological stripes, a more well-established relationship has existed between communist nations, particularly Cuba, and the traffic in illegal drugs. The same is true of the Islamic fundamentalist regime of the Taliban in Afghanistan, who controlled much of the heroin trade prior to their overthrow in 2001. Some of this activity, especially that of nongovernmental entities, falls under the category of narcoterrorism, defined by the Drug Enforcement Administration (DEA) as terrorism undertaken by groups directly or indirectly involved in producing, transporting, or distributing illegal drugs.

Whereas authoritarian and totalitarian governments deal harshly with drug traffickers inside their borders, selling drugs to Western nations serves a number of purposes. On the most basic level, it funds the activities of

revolutionary armies and terrorist groups such as al-Qaeda, or the Havana-aligned FARC rebels in Colombia. The drug trade also forces liberal democracies to allocate additional resources toward a “war on drugs,” and, by encouraging the behaviors associated with drug use, ultimately exerts a deleterious effect on the fabric of society. In such a way, encouragement of crime in a liberal democracy is a form of covert operation on behalf of an enemy state or movement.

**Intelligence and crime prevention in Democracies.** Ironically, the relationship between intelligence and crime prevention in open societies is more difficult to demonstrate. In part, this is because CIA and other organizations have far less influence on daily life in the United States than do intelligence organizations within a highly controlled political system. Still, the link between hostile governments or movements on the one hand, and crime on the other, has led U.S. authorities to increasingly link crime prevention and intelligence.

This is particularly so in the post-September 2001 world, in which the relationship between Islamist fundamentalist terrorism and the heroin trade has been clearly established. Even before that time, however, the CIA and FBI were working together and expanding operations overseas, in an effort to battle narcoterrorism. According to an April 1995 report in the *New York Times*, both agencies, along with the federal government, had begun to treat global crime as a national security issue.

The CIA has also taken an interest in crime-prevention tactics of domestic law enforcement. This is true not just on a federal level, but even—in the case of a New York City program—on a municipal level. In November 1999, CIA director George Tenet visited police headquarters in lower Manhattan to observe the operations of Compstat, a computerized statistical program whereby the New York Police Department monitors crime block by block. According to the *New York Times*, the agency was considering use of such a system to monitor entire foreign nations as a means of predicting potential unrest.

#### ■ FURTHER READING:

##### PERIODICALS:

Blair, Jayson. “C.I.A. Chief Slips in to Study Police Department Program.” *New York Times*. (November 6, 1999): section B, p. 2.

Gedda, George. “CIA Probes Cuban Link to Drug Trade.” *Associated Press*. August 16, 1999.

Johnston, David. “Strength Is Seen in a U.S. Export: Law Enforcement.” *New York Times*. (April 17, 1995): A1.

Kushner, Harvey W. “Can Security Measures Stop Terrorism?” *Security Management* 40, no. 6 (June 1996): 132.

##### SEE ALSO

*Customs Service, United States*

DEA (Drug Enforcement Administration)  
 FBI (United States Federal Bureau of Investigation)

---

## Critical Infrastructure

---

Critical infrastructure is a general term for physical and computer-based systems essential to the functions of the government and economy. Among these are telecommunications, energy, banking and finance, transportation, water systems, and emergency services. The expression *critical infrastructure* entered the language of policymakers in the mid-1990s, as it became increasingly apparent that the United States depended on a network of systems that collectively constituted its physical engine, and that these systems were potentially as vulnerable as they were valuable.

**Components of critical infrastructure.** Included under the heading of critical infrastructure are highways, airports and aircraft, trains and railways, bus lines, shipping and boat lines, transport, trucking systems, and supply networks for basic goods, electric power plants and lines, along with oil and gas lines and utilities of all kinds, including water and sewer systems, land and cell phone systems, computer networks, television, and radio (not only that which is publicly accessible, but that controlled by private or government entities in special networks or on special frequencies), banks and other financial institutions, and security, fire, hospital, and emergency services.

Each element of critical infrastructure is so vital that if it were removed from the equation, even temporarily, the entire nation would experience monumental repercussions. Even when the infrastructure of a particular area is threatened, the results can be disastrous. To this day, people alive at the time remember the northeastern electrical blackout of 1965, or the New York City blackout of 1977. Today, the critical systems that run the engine of America are far more interlinked than they were even in the 1970s, and this interdependence carries with it new vulnerabilities.

**Responding to the challenge.** Recognition of these vulnerabilities led to the creation of the President's Commission on Critical Infrastructure Protection and the Critical Infrastructure Assurance Office, as well as the integration of critical infrastructure elements of disparate departments and agencies at the federal level. It has also led to the creation of critical infrastructure protection offices by state and local governments, and by the U.S. private sector. In other parts of the industrialized world, such as Canada, concerns over critical infrastructure have led to the establishment of new departments and offices.

Protection of critical infrastructure in the United States became even more of an issue after the September 11, 2001, terrorist attacks. Though some of the measures taken have invoked the ire of civil libertarians who decry the loss of information access, and limitations on movement, faced by ordinary citizens, it is likely that the future will see even more stringent protections over the systems critical to the functioning of modern America.

### ■ FURTHER READING:

#### BOOKS:

Cordesman, Anthony H., and Justin G. Cordesman. *Cyber-Threats, Information Warfare, and Critical Infrastructure Protection: Defending the U.S. Homeland*. Westport, CT: Praeger, 2002.

*Critical Foundations: Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection*. Washington, D.C.: The Commission, 1997.

Zukin, Sharon. *Landscapes of Power: From Detroit to Disney World*. Berkeley: University of California Press, 1991.

#### PERIODICALS:

Ingram, Gregory. "Roundtable Discussion: Critical Issues in Infrastructure in Developing Countries." *Work Bank Research Observer* (1993): 473.

Lukasik, S. J., J. T. Goldberg, and S. E. Goodman. "Protecting an Invaluable and Ever-Widening Infrastructure." *Association for Computing Machinery* 41, no. 6 (June 1998): 11–16.

Robinson, C. Paul, Joan B. Woodward, and Samuel G. Varnado. "Critical Infrastructure: Interlinked and Vulnerable." *Issues in Science and Technology* 15, no. 1 (fall 1998): 61–67.

#### ELECTRONIC:

Partnership for Critical Infrastructure Security. <<http://www.pcis.org>> (February 27, 2003).

#### SEE ALSO

*Critical Infrastructure Assurance Office (CIAO), United States*

---

## Critical Infrastructure Assurance Office (CIAO), United States

---

Created by Presidential Decision Directive 63 (PDD 63) in 1998, the Critical Infrastructure Assurance Office (CIAO) of the United States Department of Commerce (DOC) has the responsibility of coordinating security for energy, financial services, transportation, telecommunications, and other



A view of chain-locked gates leading to an area of critical infrastructure, the underground Pentagon near Founatin Dale, Pennsylvania. The facility was built inside a mountain as a second central command structure if needed during wartime. AP/WIDE WORLD PHOTOS.

major systems at the federal level. After the terrorist attacks of September 11, 2001, its mission became even more critical to national security, and in early 2003 it was incorporated into the newly created Department of Homeland Security (DHS).

In May 1998, President William J. Clinton signed PDD 63. The latter called for new measures to protect critical infrastructures, which it defined as those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems, and emergency services, both governmental and private.

Among the specific policy measures of PDD 63 was the creation of CIAO, a section of DOC designed to have a life span of three years. During that time, CIAO would conduct a study of the federal government's dependence on, and vulnerabilities with regard to, critical infrastructures.

CIAO continued to exist beyond the term of its mandate, and three and a half years after its creation, its

mission gained new impetus in the wake of the September 2001 terrorist attacks. On October 16, 2001, President George W. Bush signed Executive Order 13231, "On Critical Infrastructure Protection," which established the Critical Infrastructure Protection Board (CIPB), and appointed the director of CIAO as a member of both the board and its coordination committee. On March 1, 2003, CIAO was moved from DOC to the newly created DHS.

#### ■ FURTHER READING:

##### PERIODICALS:

- Frank, Diane. "Cybersecurity Center Takes Shape." *Federal Computer Week* 16, no. 4 (February 18, 2002): 10.  
 Piazza, Peter. "Sunset of the CIAO? Industry May Decide." *Security Management*. 44, no. 11 (November 2000): 36.

##### ELECTRONIC:

- Critical Infrastructure Assurance Office. <<http://www.ciao.gov>> (January 28, 2003).

## SEE ALSO

*Commerce Department Intelligence and Security Responsibilities, United States*  
*Critical Infrastructure Assurance Office (CIAO), United States*  
*Infrastructure Protection Center (NIPC), United States National*

## Croatia, Intelligence and Security

Following World War I, the ethnic nations in the Balkan region were unified into a single state, known after 1929 as Yugoslavia. Tensions between the various ethnic populations remained high, and the government unstable. After World War II, Marshal Tito, who established a strong-handed communist dictatorship, seized the Yugoslav government. The Yugoslavian governmental intelligence was dominated by secret police forces and government-backed political espionage. Modeled after intelligence and security forces in the Soviet Union, Yugoslav intelligence focused on protecting the ruling regime under the direct control of the Communist Central Committee.

In the 1990s, Yugoslavia broke apart following the fall of the Soviet Union. Croatia was the first province to declare its independence in 1991. Border disputes and ethnic tensions flared in the region, sparking intense warfare. When fighting eased after the intervention of UN peacekeepers, Croatia began its struggle to overcome the legacy of decades of communist dictatorship. The intelligence community was a primary target of initial reforms. Though the old secret police were disbanded, and new agencies sought to distance themselves from the legacy of their predecessors, the process of rebuilding intelligence and security services continues to be problematic in Croatia.

Between 1990 and 2003, the Croatian intelligence community altered its structure several times. As of 2003, twelve departments, in two government ministries, comprise the Croatian intelligence services. The main civilian agency, under the direction of the Ministry of the Interior, is the Croatian Intelligence Service (HIS). HIS operations deal exclusively with the collection and analysis of foreign intelligence. However, the agency also performs the bureaucratic function of coordinating the efforts of all civilian intelligence operations, and processing information gathered by various agencies for dissemination to government officials.

Aiding the HIS with coordination of intelligence operations is the National Security Office (UNS). The UNS also distributed necessary intelligence information to the

government and oversees the operations of various intelligence agencies in Croatia. The UNS further coordinates joint efforts between the intelligence and law enforcement communities to act neutralize potential threats to national security. Many of Croatia's specific intelligence units, such as Communications Intelligence and Counter-intelligence force, are subsidiaries of the UNS.

A small agency, the Security Intelligence Service (OBS), conducts intelligence operations against neighboring Balkan nations, most especially Serbia and Montenegro. The agency constantly provides other intelligence and security forces with information on regional ethnic tensions, arms trafficking and stockpiling by various groups, and the strength and operations of other regional intelligence services.

The Croatian military, under the direction of the Ministry of Defense, also maintains specially trained intelligence forces, embedded in the each service branch. The small Croatian Navy collects signals, communications, and remote intelligence. The significantly larger Army Intelligence Force aids civilian intelligence operations, as well as collects information on foreign militaries. Both military and civilian intelligence forces are charged with the preservation of national security and the protection of Croatian government officials at home and abroad.

Even after U.N. intervention in the Balkan Peninsula, sporadic fighting between rival ethnic interests, and diplomatic disagreements between Croatia and neighboring states, remain endemic. Croatian government and economic reforms have made the nation the strongest in the region, with increasing participation in international organizations.

### ■ FURTHER READING :

#### ELECTRONIC:

Central Intelligence Agency. *The World Factbook, 2002.* "Croatia" <<http://www.cia.gov/cia/publications/factbook/geos/hr.html>>; (March 30, 2003).

#### SEE ALSO

*Cold War (1945–1950), The Start of the Atomic Age*  
*Cold War (1950–1972)*  
*Cold War (1972–1989): The Collapse of the Soviet Union*  
*World War I*  
*World War II*

## Cruise Missile

Cruise missiles come in several varieties, the most well known being the Tomahawk. Operating rather like a



The destroyer USS *Porter* (DDG78) launches a Tomahawk Land Attack Missile toward Iraq on March 22, 2003, during Operation Iraqi Freedom; the missile struck a government communications site in Baghdad. AP/WIDE WORLD PHOTOS.

pilotless airplane, these missiles have powerful guidance systems that make them capable of hitting precise targets from a great distance. Operated by the United States Air Force and Navy, cruise missiles can be deployed from aircraft, submarines, and destroyers.

Of the two most notable types of cruise missile, the Tomahawk, most often used by the Navy, is 18 feet, 3 inches (5.56 m) long and weighs 2,900 pounds (1,315 kg). The Air Force AGM-86B/C weighs 3,150 pounds (1,429 kg) and measures 20 feet, 9 inches (6.3 m). The AGM, first deployed (as an 86B) in December 1982, is an air-to-ground strategic cruise missile, while the Tomahawk, which first saw service in 1986, is a long-range subsonic cruise missile for striking high-value or heavily defended land targets. Both have gone through several changes, including the introduction of the Tactical Tomahawk, to be launched from forward-deployed ships and submarines, in 2004.

A cruise missile includes a solid rocket booster, which makes up approximately fifteen percent of its weight at

launch. Once it has burned its fuel, the booster falls away and the missile's wings, tail fins, and air inlet unfold. From that point until it reaches its target, the missile is powered by its turbofan engine. In flight, the cruise missile has a speed of about 550 miles per hour (880 kph).

Neither size nor speed nor rocket booster systems define the cruise missile as much as its accuracy. The Tomahawk has a range of 870 nautical miles (1,000 statute miles, or 1,609 km), and the AGM more than 1,500 miles (2,400 km) or more—the exact figure is classified—yet both are capable of hitting a target the size of a truck. Guiding these missiles are four different systems: the inertial guidance system, which detects changes in the missile's motion; terrain contour matching, which applies a three-dimensional database of the terrain over which the missile flies; global positioning system (GPS), which includes both military satellites and an onboard GPS receiver; and digital scene matching area correlation, which switches on once the missile nears its target, using an image correlator and a camera to locate the target.



## ■ FURTHER READING:

### BOOKS:

Gormley, Dennis. *Dealing with the Threat of Cruise Missiles*. New York: Oxford University Press for the International Institute for Strategic Studies, 2001.

Huisken, Ronald. *The Origin of the Strategic Cruise Missile*. New York: Praeger Publishers, 1981.

Werrell, Kenneth P. *The Evolution of the Cruise Missile*. Maxwell Air Force Base, AL: Air University Press, 1985.

### ELECTRONIC:

Fact Sheet: AGM-86B/C Missiles. U.S. Air Force. <[http://www.af.mil/news/factsheets/AGM\\_86B\\_C\\_Missiles.html](http://www.af.mil/news/factsheets/AGM_86B_C_Missiles.html)> (April 7, 2003).

How Cruise Missiles Work. Howstuffworks.com. <<http://www.howstuffworks.com/cruise-missile.htm>> (April 7, 2003).

Navy Facts: Tomahawk Cruise Missile. U.S. Navy Office of Information. <<http://www.chinfo.navy.mil/navpalib/factfile/missiles/wep-toma.html>> (April 7, 2003).

### SEE ALSO

*Ballistic Missiles*

*Ballistic Missile Defense Organization, United States*

*GPS*

*Patriot Missile System*

*Strategic Defense Initiative and National Missile Defense Undersea Espionage: Nuclear vs. Fast Attack Subs*

## Cryo3 Detector.

SEE *Lawrence Berkeley National Laboratory*.

# Cryptology and Number Theory

## ■ K. LEE LERNER

Cryptography is a division of applied mathematics concerned with developing schemes and formula to enhance the privacy of communications through the use of codes. More specifically, cryptography is the study of procedures that allow messages or information to be encoded (obscured) in such a way that it is extremely difficult to read or understand encoded information without having a specific key (i.e., procedures to decode) that can be used to reverse the encoding procedure.

Cryptography allows its users, whether governments, military, businesses or individuals, to maintain privacy and confidentiality in their communications. The goal of every cryptographic scheme is to be "crack proof" (i.e., only able to be decoded and understood by authorized recipients). Cryptography is also a means to ensure the

integrity and preservation of data from tampering. Modern cryptographic systems rely on functions associated with advanced mathematics, number theory that explores the properties of numbers and the relationships between numbers.

Encryption systems can involve the simplistic replacement of letters with numbers, or they can involve the use of highly secure "one-time pads" (also known as Vernam ciphers). Because one-time pads are based upon codes and keys that can only be used once, they offer the only "crack proof" method of cryptography known. The vast number of codes and keys required, however, makes one-time pads impractical for general use.

Many wars and diplomatic negotiations have turned in the ability of one combatant or country to read the supposedly secret messages of its enemies. The use of cryptography has broadened from its core diplomatic and military users to become of routine use by companies and individuals seeking privacy in their communications. Governments, companies and individuals required more secure systems to protect their databases and email.

In addition to improvements made to cryptologic systems based on information made public from classified government research programs, international scientific research organizations devoted exclusively to the advancement of cryptography (e.g., the International Association for Cryptologic Research (IACR)), began to apply applications of mathematical number theory to enhance privacy, confidentiality, and the security of data. Applications of number theory were used to develop increasingly involved algorithms (i.e., step-by-step procedures for solving a mathematical problems). In addition, as commercial and personal use of the Internet grew, it became increasingly important, not only to keep information secret, but also to be able to verify the identity of message sender. Cryptographic use of certain types of algorithms called "keys" allow information to be restricted to a specific and limited audiences whose identities can be authenticated.

## Mathematical Operations

In some cryptologic systems, encryption is accomplished, for example, by choosing certain prime numbers and then products of those prime numbers as a basis for further mathematical operations. In addition to developing such mathematical keys, the data itself is divided into blocks of specific and limited length so that the information that can be obtained even from the form of the message is limited. Decryption is usually accomplished by following an elaborate reconstruction process that itself involves unique mathematical operations. In other cases, decryption is accomplished by performing the inverse mathematical operations performed during encryption.

In the late 1970s, government intelligence agencies and Ronald Rivest, Adi Shamir, and Leonard Adleman published an algorithm (the RSA algorithm) destined to become a major advancement in cryptology. The RSA

algorithm underlying the system derives its security from the difficulty in factoring very large composite numbers. The RSA algorithm was the mathematical foundation for the development of a public two-key cryptographic system called Pretty Good Privacy (PGP).

Applications of number theory allow the development of mathematical algorithms which can make information (data) unintelligible to everyone except for intended users. In addition, mathematical algorithms can provide real physical security to data—allowing only authorized users to delete or update data. One of the problems in developing tools to crack encryption codes involves finding ways to factor very large numbers. Advances in applications of number theory, along with significant improvements in the power of computers, have made factoring large numbers less daunting.

In general, the larger the key size used in a system, the longer it will take computers to factor the composite numbers used in the keys.

Specialized mathematical derivations of number theory such as theory and equations dealing with elliptical curves are also making an increasing impact on cryptology. Although, in general, larger keys provide increasing security, applications of number theory and elliptical curves to cryptological algorithms allow the use smaller keys with any loss of security.

Advancements in number theory are also used to crack important cryptologic systems. Attempting to crack encryption codes (the encryption procedures) often requires use of advanced number theories that allow, for instance, an unauthorized user to determine the product of the prime numbers used to start the encryption process. Factoring this product is, at best, a time consuming process to determine the underlying prime numbers. An unsophisticated approach, for example, might be to simply attempt or apply all prime numbers. Other more elegant attempts involve algorithms termed quadratic sieves, a method of factoring integers, developed by Carl Pomerance, that is used to attack smaller numbers, and field sieves algorithms that are used in attempts to determine larger integers. Advances in number theory allowed factoring of large numbers to move from procedures that, by manual manipulation, could take billions of years, to procedures that—with the use of advanced computing—can be accomplished in weeks or months. Further advances in number theory may lead to the discovery of a polynomial time factoring algorithm that can accomplish in hours what now takes months or years of computer time.

Advances in factoring techniques and the expanding availability of computing hardware (both in terms of speed and low cost) make the security of the algorithms underlying cryptologic systems increasingly vulnerable.

These threats to the security of cryptologic systems are, in some regard, offset by continuing advances in design of powerful computers that have the ability to generate larger keys by multiplying very large primes. Despite the advances in number theory, it remains easier

to generate larger composite numbers than it is to factor those numbers.

Other improvements related to applications of number theory involve the development of “non-reputable” transactions. Non-reputable means that parties can not later deny involvement in authorizing certain transactions (e.g., entering into a contract or agreement). Many cryptologists and communication specialists assert that a global electronic economy is dependent on the development of verifiable and non-reputable transactions that carry the legal weight of paper contracts. Legal courts around the world are increasingly faced with cases based on disputes regarding electronic communications.

#### ■ FURTHER READING:

##### BOOKS:

Burn R. P. *A Pathway into Number Theory*, 2nd. ed. New York: Cambridge University Press, 1997 .

Niederreiter, Harald. *Mathematical Foundations of Coding and Cryptology*. Singapore: World Scientific Press, 2003 .

Wagstaff, Samuel S., Jr., *Cryptanalysis of Number Theoretic Cyphers* Boca Raton, FL: CRC Press, 2002 .

##### SEE ALSO

*Cryptology, History*  
*Cryptonym*

---

## Cryptology, History

---

#### ■ JUDSON KNIGHT

Cryptology is the study of both cryptography, the use of messages concealed by codes or ciphers, and cryptanalysis, or the breaking of coded messages. It is nearly as old as civilization itself, although ciphers and codes prior to the late medieval period in western Europe tended to be extremely simple by today’s standards. Advances in mathematics made possible the development of ever more sophisticated systems. Further improvements in cryptology accompanied the creation of modern standing armies and intelligence services during the nineteenth century. Following the world wars and the creation of the computer, cryptology entered a far more advanced stage, resulting in the creation of codes and ciphers so sophisticated that virtually no amount of human genius unaided by computer technology can break them.

### Ancient Cryptology

Early examples of cryptology can be found in the work of Mesopotamian, Egyptian, Chinese, and Indian scribes. In those four cradles of civilization, which emerged during



Cryptography on display at the National Cryptologic Museum in Ft. Meade, Maryland. ©RUBIN STEVEN/CORBIS SYGMA.

the period between 3500 and 2000 B.C., few people could read and write, therefore, written language was a secret code in itself. Further concealment of meaning behind opaque hieroglyphs, cuneiform, or ideograms served to narrow the intended audience even further.

The specialization of writing skills served, in two cases, to prevent the transmission of these skills to later generations. Knowledge of hieroglyphic writing in Egypt died out, and without the discovery and deciphering of the Rosetta Stone in the early nineteenth century, translation of Egyptian texts would probably have not occurred until the computer age—if at all. The fact that the written language of the Indus River valley civilizations in ancient India remains to be translated serves as proof that computers cannot solve all cryptologic questions without a crib or key.

**Greece and Rome.** Modern scholars know a great deal more about cryptologic systems in Greece and Rome than in earlier civilizations. The Spartans in about 400 B.C. used a cryptographic system called a *scyta/e*, whereby a sheet of

papyrus was wrapped around a staff, a message was written down the length of the staff, and then the papyrus was unwrapped. In order to read the message properly, the recipient had to have a staff of exactly the same diameter.

Two centuries later, the Greek historian Polybius introduced what became known as the Polybius square, a 5 x 5 grid that used the 24 letters of the Greek alphabet—a model for the ADFGX cipher used by the Germans in World War I. Julius Caesar in the first century B.C. employed one of the first known ciphers, a system that involved a shift three letters to the right: for example, a plain text *Z* would become a *C*, an *A* a *D*, and so on.

## Medieval Cryptology

Progress in cryptology—as with most other areas of study—came to a virtual standstill between the decline of the Roman Empire in the third century and the rise of Islam in the seventh. Arab scholars pioneered cryptanalysis, the solving of ciphers or codes without the aid of a key, from the eighth century onward. In 1412, al-Kalka-shandi published a treatise in which he introduced the technique, later made famous to popular audiences by Edgar Allan Poe in “The Gold Bug,” of solving a cipher based on the relative frequency of letters in the language.

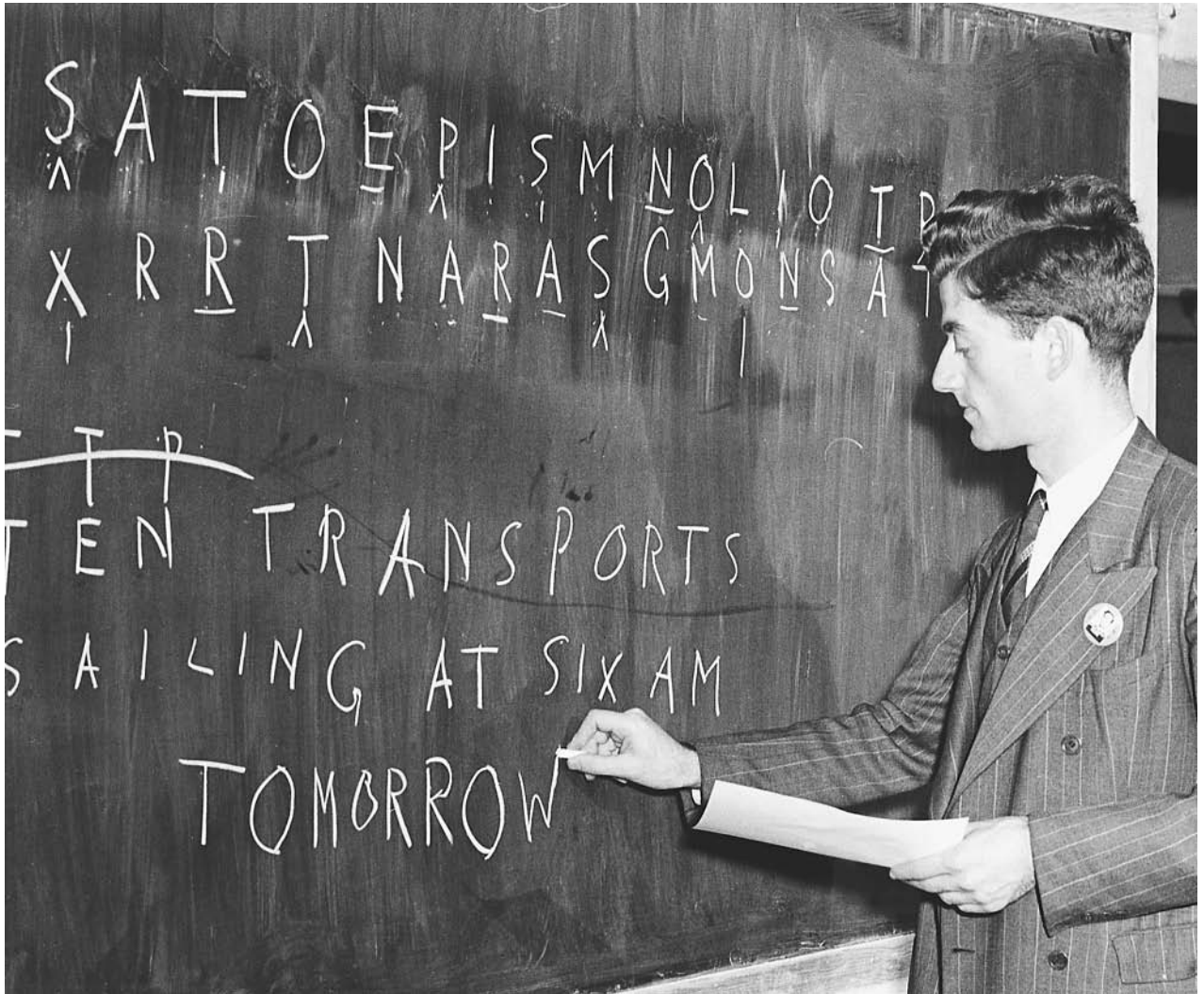
By that time, cryptology had begun to advance again in Europe, where the Italian city states used secret codes for their diplomatic messages in the fourteenth century. Messages were carried on horseback, and even in peacetime, the roads of Europe were plagued with highway robbers, so secrecy in communication was of the utmost importance.

Progress in mathematical learning from the twelfth century onward aided these advances. In the early thirteenth century, Italian mathematician Leonardo Fibonacci introduced the Fibonacci sequence, wherein each number is the sum of the previous two: 1, 1, 2, 3, 5, 8, and so on. Fibonacci’s sequence would prove highly influential in cryptology: even in the late twentieth century, some cryptologic systems relied on an electronic machine called a Fibonacci generator, which produced numbers in a Fibonacci sequence.

In the late fifteenth century, another influential Italian mathematician, Leon Battista Alberti, published a work in which he introduced the idea of a cipher disk. The latter is a device for encoding and decoding messages by use of concentric wheels imprinted with alphabetic and numeric characters. Even in the late nineteenth century, cryptographers were using cipher disks based on the model pioneered by Alberti.

## The Early Modern Era (1500–1900)

Due to its secret nature, cryptography—a word based on Greek roots meaning “secret writing”—had long been



This worker in the office of postal censorship in New York City, in 1942, deciphers a coded message found in a letter. ©BETTMANN/CORBIS.

associated with the occult, and one occultist who advanced the art was the early sixteenth-century German monk Trithemius. Trithemius developed a table in which each row contained all the letters of the alphabet, but each successive row was shifted over by one letter. The first letter of plain text would be encrypted using the first line, the second letter using the second line, and so on. Late in the 1500s, French cryptographer Blaise de Vigenère adapted the Trithemius table for his own Vigenère table, which in the twentieth century became the basis for the widely used data encryption standard, or DES.

By the eighteenth and early nineteenth centuries, cryptography had become widely used in Europe, where governments employed special offices called “black chambers” to decipher intercepted communications. In America, Thomas Jefferson developed an early cipher wheel, and in the 1840s, Samuel F. B. Morse introduced a machine that would have a vast impact on cryptology: the telegraph. Up to this time, all encoded or enciphered

communication had been written and carried by hand, and the telegraph marked the first means of remote transmission. It also employed one of the most famous codes in the world, the Morse code, and helped influence widespread popular interest in cryptography. (It is no accident that Poe’s fictional writing on cryptology coincided with this era.)

In the 1850s, Charles Wheatstone and Lyon Playfair introduced the Playfair system, which used a Polybius square and encrypted letters in pairs. This pairing made deciphering more difficult, since it was less easy to see how frequently certain letters appeared. The Playfair system proved so effective that the Allies used it in limited form against the Japanese during World War II. Despite these advances of the era, cryptography was still far from advanced during the American Civil War. The Confederacy was so disadvantaged in the realm of cryptanalysis that its government sometimes published undeciphered Union messages in newspapers with a request for readers’ help in deciphering them.



A Korean War veteran examines a display explaining how cryptology was used to intercept North Korean radio transmissions during the Korean War at the National Cryptologic Museum in Ft. Meade, Maryland. AP/WIDE WORLD PHOTOS.

## The Twentieth Century

In the early twentieth century, another invention, the radio, had a profound effect on cryptography by greatly improving the capacity of senders to transmit messages to remote areas. World War I marked a watershed in cryptography. Not only was it the first major conflict in which radio was used, it was the last in which a great power failed to employ cryptographic communications. On the Eastern Front, the Russians sent uncoded messages that were easily interpreted by Russian-speaking intelligence officers on the German and Austrian side,

leading to a massive victory for the Central Powers at Tannenberg in 1914.

The war also marked the debut of the Germans' ADFGX cipher, which was so sophisticated that French cryptanalysts only deciphered it for one day, after which the Germans again changed the key. But the cryptographic dimension of the war did not belong entirely to the Central Powers. British signal intelligence cracked the German cipher, and intercepted a message from German foreign minister Arthur Zimmermann to the Mexican president, promising to return territories Mexico had lost to the

United States in the Mexican War if the country attacked the United States. Informed of the Zimmermann telegram, President Woodrow Wilson declared war on Germany.

Also in 1917, American engineer Gilbert S. Vernam developed the first significant automated encryption and decryption device when he brought together an electromagnetic ciphering machine with a teletypewriter. A year later, Major Joseph O. Mauborgne of the U.S. Army devised the one-time pad, whereby sender and receiver possess identical pads of cipher sheets that are used once and then destroyed—a virtually unbreakable system. World War I also saw the development of a cipher machine by Edward Hebern, who tried to sell his idea to the U.S. Navy. The Navy rejected Hebern's system, which was later taken by the Japanese and used in World War II. By the time of that war, Hebern had developed Mark II (SIGABA), which became the most secure U.S. cipher system during the conflict.

Allied cryptologic victories against the Axis in World War II have long been celebrated in the intelligence community, and few have received more acclaim than the cracking of the German Enigma code. The Germans' Enigma machine, invented by German electrical engineer Arthur Scherbius around the same time Hebern introduced his device, was a complex creation in which the variable settings of rotors and plugs determined the keys. Solving it was a major victory for the Allies, who kept secret the fact that they had cracked the system so as to keep exploiting it. Cracking of codes also aided victories in North Africa and the Pacific. At the same time, American use of codetalkers transmitting enciphered messages in the Navajo Indian language made their transmissions indecipherable to the Japanese.

**The computer age.** American cryptologic work during World War II had contributed to the development of a machine, the computer, which would revolutionize cryptology to an even greater extent than the telegraph or radio had previously. Most cryptologic advances since the war have involved, or made use of, computers. A quarter-century after the war's end, in the early 1970s, American electrical engineers Martin Hellman and Whitfield Diffie introduced the idea of asymmetric or public-key ciphers, which are extremely hard to crack. This led to the development of the RSA algorithm (named for its creators, Rivest, Shamir, and Adelman) at the Massachusetts Institute of Technology in 1977.

Also in 1977, the U.S. federal government introduced DES, a transposition-substitution algorithm so complex that it seemed a safe means of guarding computer data. Given the fact that DES had some  $2^{56}$  possible keys (a number roughly equivalent to a 1 followed by 17 zeroes), it had seemed unbreakable at the time. By the early 1990s, however, vast increases in the processing speed of computers had made it possible for hackers to break DES using "brute-force" means—that is, trying every possible value

for a given cipher until finding a solution. To guard against these attacks, new Advanced Encryption Standard (AES) algorithms were developed to replace DES.

Advances in computers, and in communication by electronic means over the Internet, have both enabled and necessitated progress in cryptology. For example, electronic commerce requires sophisticated encryption systems to protect users' credit card information. Similarly, digital communication via cellular telephones requires encryption to prevent easy interception of phone calls. Developments of the 1990s include Phil Zimmermann's PGP (Pretty Good Privacy) to protect e-mail communications.

#### ■ FURTHER READING:

##### BOOKS:

- Beutelspacher, Albrecht. *Cryptology: An Introduction to the Art and Science of Enciphering, Encrypting, Concealing, Hiding, and Safeguarding Described Without Any Arcane Skulduggery But Not Without Cunning Waggyery for the Delectation and Instruction of the General Public*. Washington, D.C.: Mathematical Association of America, 1994.
- Haldane, Robert A. *The Hidden War*. New York: St. Martin's Press, 1978.
- Kahn, David. *Kahn on Codes: Secrets of the New Cryptology*. New York: Macmillan, 1983.
- Konheim, Alan G. *Cryptography, a Primer*. New York: Wiley, 1981.
- Lubbe, J. C. A. van der. *Basic Methods of Cryptography*. New York: Cambridge University Press, 1995.
- Melton, H. Keith. *The Ultimate Spy Book*. New York: DK Publishing, 1996.

##### SEE ALSO

- ADFGX Cipher*  
*Cryptology and Number Theory*  
*GSM Encryption*  
*Pretty Good Privacy (PGP)*

---

## Cryptonym

---

Cryptonym, or code names, are words, symbols, or numbers used in place of the actual name of a person, item, or planned event. The term is derived from two Latin roots, *crypto* meaning secret, and *nym*, meaning name. A security and counterintelligence measure, code names facilitate covert communication and enhance secrecy.

Cryptonym have long existed in many forms, each tailored to fit the circumstance in which they are used. To preserve security, military and intelligence operation code

names most often have little or no relationship to the classified item, person, or event that they represent. Sometimes, such cryptonym are intentionally misleading. During World War II, the American military used the code name “Husky” to refer to a planned 1943 invasion of North Africa.

Intelligence and military agents working in the field often use cryptonym to disguise their identity. As means of protecting both volunteer operatives and the organizations, members of partisan groups in the French Resistance referred to each other by code names. Names of French villages, historical persons, and professional titles were commonly used cryptonym. Resistance volunteers adhered to the codename system to minimize the chance of Gestapo infiltrators, or with captured partisans under duress, easily identifying organization members.

Other types of cryptonym include number series, now commonly used in reference to military and computer technology, and symbols. Though used extensively throughout history as a means of maintaining a secret identity, the practice of substituting secret symbols for proper names has fallen out of favor. In medieval France and England, knights and nobles wishing to send secret communications often signed their messages with secretive wax seals different in color and design from their family crests or signature seals.

Although assigning intelligence matters of great importance a cryptonym is one of the oldest espionage and enciphering technologies, the practice remains commonplace today. Code names are no longer the exclusive domain of governments, military, or intelligence agencies. With the advent of the Internet, the ever-present user name, or handle, has become the most popularly used form of cryptonym.

#### SEE ALSO

*Code Word*

## CT Scanners.

SEE *Scanning Technologies*.

## Cuba, Intelligence and Security

Cuba has a security and intelligence apparatus that, when considered in light of the nation’s size and its weak economy, is on a scale many times larger than that of the United States. Whereas its poverty, lack of exports, and

depressed economic conditions would normally make Cuba an irrelevant player on the international scene, its clandestine operations extend its influence throughout the globe.

Chief among Cuban intelligence agencies is the Dirección General de Inteligencia (DGI), or General Intelligence Directorate. Established within the Ministry of the Interior in 1961, DGI initially took an aggressive role in fomenting third-world Communist revolutions. By the late 1960s, however, Cuba’s Soviet sponsors had grown wary of this adventurism, and pressured Castro to purge DGI leadership. Thereafter the agency focused on intelligence collection.

**Operations against the United States.** Today DGI collects a wide variety of data through its operatives in Europe, the Third World, and North America—especially the last of these, because the United States is Cuba’s self-declared number-one foe. The Cuban delegation to the United Nations in New York City is the third-largest in the world, and it has been estimated that nearly half of its personnel are DGI officers. In 1982, United States authorities convicted four Castro aides of smuggling drugs into the United States, and subsequently uncovered a vast drug-smuggling ring that operated in cooperation with General Manuel Noriega’s Panama, as well as with Colombian drug lords.

Over a period of five years beginning in 1998, the Federal Bureau of Investigation (FBI) uncovered a Florida spy ring consisting of at least 16 Cuban operatives. They functioned on a shoestring budget, and had to account to Havana for money spent, but in the realm of spying at least, Castro’s regime often manifests what analysts contend is a certain economic genius. In some cases, Havana receives intelligence free of cost. Ana B. Montes, a senior intelligence analyst at the Pentagon arrested in September 2002, received no money for activities on behalf of Cuba. Referring to the United States economic embargo against Cuba, in force since 1961, Montes claimed her actions reflected her concern over allegations of Washington’s alleged unfair treatment of the Castro regime.

After the DGI reorganization, responsibility for “national liberation movements” shifted to the National Liberation Directorate (DLN), that in 1974 became the America Department (DA) of the Communist Party of Cuba Central Committee. DA, which supported the Communist movements that gained control of Nicaragua and Grenada in the 1970s and 1980s, is reported to have trained and supported guerrillas and terrorists. Many of its operatives function in supposedly innocuous positions, including the diplomatic corps and Cuban-front corporations.

In addition to DGI and DA, there is the Military Counterintelligence Department of the Ministry of Revolutionary Armed Forces, which conducts counterintelligence, signals intelligence, and electronic warfare activities against the United States.

The *New York Times* called “Cuba’s intelligence apparatus the “Little Spy Engine That Could.” Despite a stagnant economy crippled by Castro’s policies—and sustained almost entirely by foreign aid and tourism—the Cubans have managed to maintain a security apparatus unequalled by that of any similarly small country other than perhaps Israel. And whereas, by comparison, Israel has a prosperous economy, Cuba has had to weather the loss of considerable aid following the collapse of the Soviet Union in the late 1908s and early 1990s. The post-Soviet Russian government has continued to offer support to its old ally, but on a much smaller scale than did its communist predecessor at the height of the Cold War.

The administration of President George W. Bush has accused Cuba of aligning itself with worldwide terrorist networks. Indeed, Castro has maintained friendly relations with all three members of what President Bush has publicly labeled the “axis of evil”: Iran, Iraq, and North Korea.

#### ■ FURTHER READING:

##### BOOKS:

Bennett, Richard M. *Espionage: An Encyclopedia of Spies and Secrets*. London: Virgin Books, 2002.

##### PERIODICALS:

Golden, Tim. “White House Wary of Cuba’s Little Spy Engine That Could.” *New York Times*. (January 5, 2003): p. 1.3.

##### ELECTRONIC:

Cuban American National Foundation. <<http://www.canfnet.org/>> (January 22, 2003).

Cuban Intelligence Agencies. Fellowship of American Scientists. <<http://www.fas.org/irp/world/cuba/index.html>> (January 22, 2003).

##### SEE ALSO

*KGB* (Komitet Gosudarstvennoi Bezopasnosti, *USSR Committee of State Security*)

---

## Cuban Missile Crisis

---

#### ■ LARRY GILMAN

The Cuban missile crisis of October 1962 was triggered by the Soviet deployment to Cuba of medium-range, nuclear-armed ballistic missiles. The United States demanded that the Soviet Union remove these missiles and imposed a naval blockade on Cuba, threatening to sink any Soviet ships that approached the island without permitting their

cargoes to be inspected. Eventually, the Soviet Union (U.S.S.R.) announced that it would remove the missiles, and the crisis ended. Most historians affirm that the world has never been closer to global nuclear war than during the 13 days of the Cuban missile crisis (Oct. 14–Oct. 28, 1962).

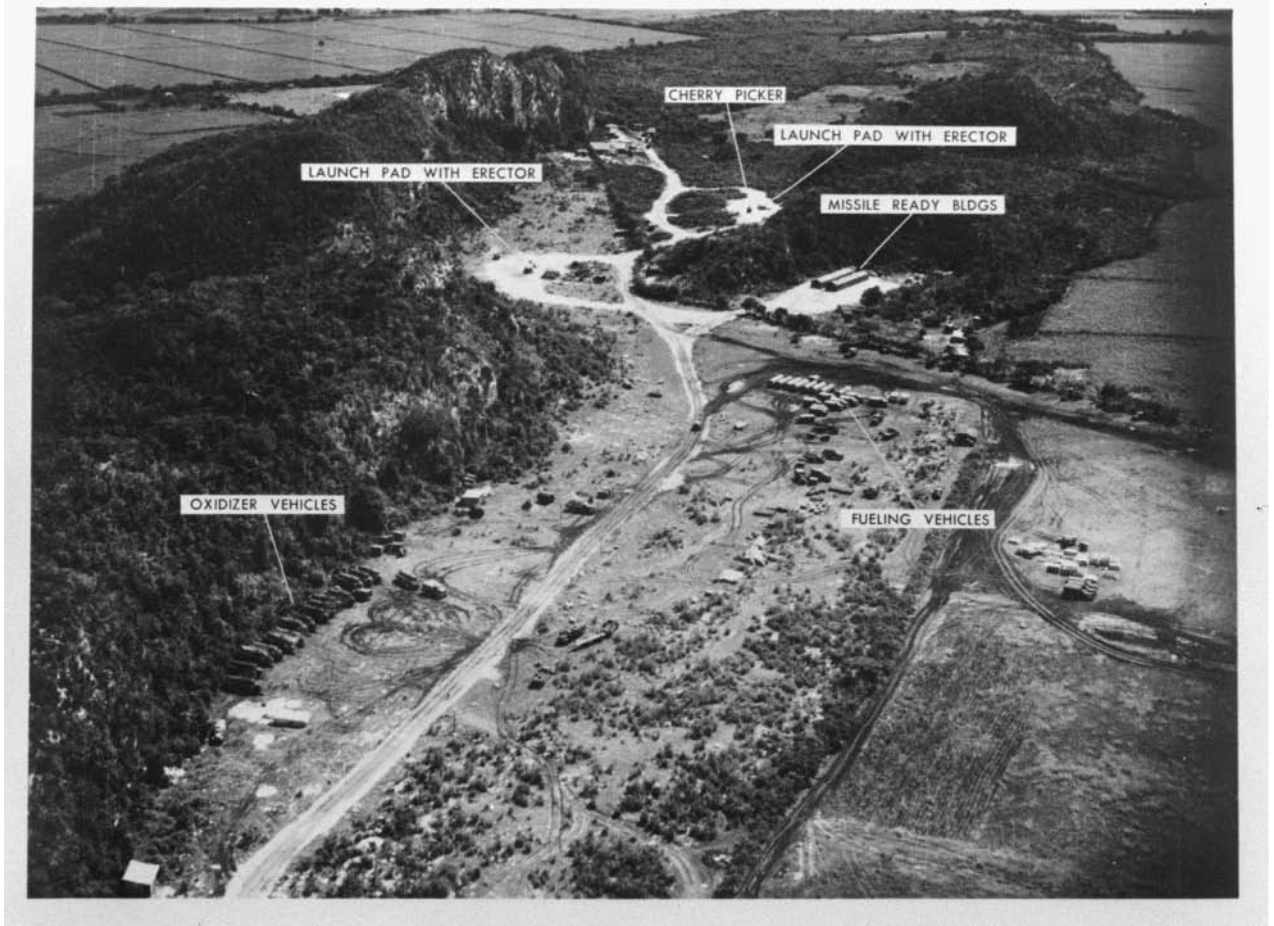
The roots of the Cuban missile crisis go back, in part, to an earlier crisis—the failed Bay of Pigs invasion of Cuba by Cuban expatriates trained, supplied, and directed by the U.S. Central Intelligence Agency. The purpose of the failed invasion was to overthrow Fidel Castro’s leftist rule of Cuba, but had two unintended effects. First, it frightened Castro, causing him to make concessions to the U.S.S.R., which wanted to place military bases on the island of Cuba, in exchange for protection against further U.S. invasion attempts. Second, it heightened tensions between the U.S. and U.S.S.R. Khrushchev, the Soviet leader, read U.S. weakness in the Bay of Pigs fiasco, and blustered publicly that he might retaliate by driving the U.S. out of West Berlin. U.S. President John Kennedy, in return, openly boasted that the U.S. possessed many more (and more accurate and deliverable) nuclear missiles and warheads than the U.S.S.R., and would consider striking first with them if it ever found itself at a military disadvantage. Kennedy’s claim was true; in 1962, the U.S.S.R. had at most 20 or 30—perhaps as few as *four*—functional, deployed intercontinental ballistic missiles (ICBMs); the U.S. had several hundred. Nevertheless, Kennedy had claimed, during his presidential campaign, that the incumbent Eisenhower’s administration had allowed the Soviets to get *ahead* of the U.S. in missiles, causing a “missile gap.” A missile gap did exist, as Kennedy knew, but in reverse; it had always been the U.S. that was far ahead of the U.S.S.R. in such weapons. Once in office, Kennedy dropped the old story about the “missile gap” and brandished the United States’s nuclear superiority openly against Khrushchev.

Khrushchev’s response was to secretly build missile bases on Cuban soil to compensate for Soviet inferiority in ICBMs. These missiles were medium-range and intermediate-range, rather than intercontinental, but from Cuba could reach the entire continental U.S. except its northwest corner. Similar missiles had been by stationed the United States for years in Turkey, which borders southern Russia. Castro gave permission to the Soviets to build Cuban missile bases in trade for a promise of protection against U.S. invasion and for cancellation of Cuban monetary debts.

Construction of the Cuban bases proceeded throughout the summer of 1962. The U.S. was aware, from various intelligence sources, that the Soviets were building up military forces on the island, but did not realize that intermediate-range nuclear weapons were part of the plan. Kennedy issued warnings to Khrushchev that the U.S. would not tolerate a major military buildup in Cuba, but would do “whatever must be done” to guarantee U.S. security; Kennedy and his advisors believed that Khrushchev would take these grave warnings seriously, and were



## MEDIUM RANGE BALLISTIC MISSILE BASE IN CUBA



A low-level photograph taken November 1, 1962, of a medium range ballistic missile site at Sagua La Grande, Cuba, showing launch erectors removed and the launchpads bulldozed over. AP/WIDE WORLD PHOTOS.

also aware that the U.S.S.R. had never yet placed nuclear weapons outside Russian territory; these factors made it seem unlikely that nuclear weapons were part of the Cuban buildup. Nevertheless, they were.

U-2 spy planes (aircraft designed to take reconnaissance photographs from very high altitudes) were making regular flights over Cuba, observing the military buildup. On October 14, a U-2 spy plane photographed an area near San Cristóbal, Cuba, revealing launch pads, missile erectors, and transport trucks for medium-range missiles. Four of the launchers were already in firing position. Khrushchev had decided to deploy launchers for at least 16 intermediate-range missiles (capable of reaching most of the continental U.S.) and 24 medium-range missiles (capable of reaching the southeastern U.S., including Washington, D.C.).

The U-2 pictures were shown to Kennedy on the morning of October 16. Much like the Kennedy administration's claims during the Bay of Pigs crisis that the U.S. had no illegal intentions in Cuba, Khrushchev's claims to

have no desire to base missiles in Cuba had proved to be untrue. Kennedy hastily assembled an ad hoc executive committee of the National Security Council, which helped him come up with two alternative plans: (1) Immediate attack on the Soviet missile sites in Cuba, followed by a full invasion of the island using 180,000 U.S. troops. (2) A naval blockade of Cuba, to be lifted only if the Soviets removed its missiles. If the blockade did not work—and it was a risky plan, as such a blockade is, by international law, an act of war—the invasion plan would be carried out.

On October 22, 1962, Kennedy addressed the American people by television. He stated:

"This sudden, clandestine decision to station strategic weapons for the first time outside of Soviet soil is a deliberately provocative and unjustified change in the status quo which cannot be accepted by this country if our courage and our commitments are ever to be trusted again. . . To halt this offensive buildup, a strict quarantine on all offensive military equipment under shipment to Cuba is being initiated. All ships of any kind bound for

Cuba from whatever nation or port will, if found to contain cargoes of offensive weapons, be turned back.”

Over the next four days, ships carrying Russian goods were searched at sea, and several Soviet vessels carrying missiles were turned back by U.S. naval vessels. The U.S. Strategic Air Command placed all its B-52 intercontinental bombers on 15-minute takeoff alert on October 20; on October 22, it placed them on a revolving airborne alert, with a percentage of bombers airborne at all times, ready to head over the North Pole toward the Soviet Union. ICBM crews were also placed on highest alert, ready to launch, and nuclear-armed Polaris submarines moved to their pre-assigned war stations at sea. The Soviet Union already had over 45,000 of its own troops on Cuba (though the U.S. estimated only 16,000), armed with 90 short-range nuclear warheads that would have been used against a U.S. invasion force. (The U.S. did not know of these short-range nuclear weapons.)

A U.S. invasion of Cuba, had it occurred, could have escalated rapidly to nuclear war, first in Cuba and then globally. The entire world, including Kennedy and Khrushchev and their advisors, feared throughout the crisis that global nuclear war was extremely probable. If nuclear war had occurred, it could have caused hundreds of millions of deaths, and significantly destroyed the U.S., the U.S.S.R., and many other nations as functioning societies.

On October 26, Khrushchev sent a private message to Kennedy indicating that he would be willing to remove the missiles if the U.S. would promise not to invade Cuba. The following day, a more formal message said that Soviet Union would remove its missiles only if the U.S. would remove its Jupiter-class intermediate-range missiles from Turkey. In secret negotiations between Soviet ambassador Anatoly Dobrynin and U.S. attorney general Robert Kennedy (brother of President Kennedy), the U.S. did promise not to invade Cuba in exchange for withdrawal of the Soviet missiles; it did not, however, promise to remove its missiles from Turkey. These missiles were considered largely symbolic by U.S. strategists, and were technically unreliable and obsolete. Additionally, their threat to the U.S.S.R. could have been replaced by deployment of a Poseidon submarine carrying nuclear missiles to the eastern Mediterranean. In secret, therefore, Kennedy seriously considered trading the missiles in Turkey for the missiles in Cuba, although in public he refused to do. On October 28—one day before the deadline urged by the U.S. Joint Chiefs of Staff for launching a Cuban invasion—the Soviets stated that they would remove their missiles from Cuba. The crisis abated.

Many historians have viewed Kennedy’s handling of the Cuban missile crisis as a masterpiece of statesmanship. The Soviet Union backed down; its missiles were removed; U.S. goals were fully met; American geomilitary prestige was preserved. Other historians argue that the Kennedy administration was not as deft in reality as it seemed publicly. Kennedy and his advisors were badly

frightened; Secretary of State Dean Rusk began to weep when told, at the height of the crisis, that a U-2 plane had been shot down over Cuba. Robert Kennedy said later that his brother had put events in motion that he could not control.

What is certain is that Khrushchev and Kennedy were both willing to risk global nuclear war for dubious gains. The Soviets were soon to achieve strategic nuclear parity with the U.S. simply by building more and better ICBMs; any strategic advantage to be gained by placing missiles in Cuba would, therefore, be short-term. By the same token, no long-term U.S. interests were at stake in the deployment of Soviet intermediate-range missiles to Cuba, as within a few years every city in the continental U.S. would be vulnerable to Soviet ICBMs and submarine-launched ballistic missiles anyway. Kennedy administration officials knew that the Soviet buildup in Cuba would, at worst, decrease the United States’s massive strategic advantage, or *appear* to do so—in Kennedy’s words, make the Soviets “look like they’re coequal with the U.S.” Kennedy was thus, willing to gamble the world’s future not to save the U.S. from an imminent military threat, but because to tolerate the Soviet buildup in Cuba would, in his words, “have politically changed the balance of power. It would have appeared to, and appearances contribute to reality.”

The U.S. emerged from the Cuban missile crisis with greatly expanded confidence in its own geopolitical skill. Its policymakers had verified, as they believed, that “showing resolve” (threatening to use military force) was more effective than diplomacy, the United Nations, or international law—with the proviso that the U.S. should be more willing to commit conventional (non-nuclear) military forces in a crisis, in order to keep back from the nuclear abyss. Today, many historians argue that U.S. willingness to invade Vietnam is directly attributable to its success during the Cuban missile crisis.

#### ■ FURTHER READING:

##### BOOKS:

Nathan, James. *Anatomy of the Cuban Missile Crisis*. Westport, CT: Greenwood Press. 2001.

##### PERIODICALS:

Frankel, Max. “Learning from the Missile Crisis.” *Smithsonian*. October, 2002: 53–64.

##### SEE ALSO

*Bay of Pigs*

## Culper Ring.

SEE *Revolutionary War, Espionage and Intelligence*.

## Cultural Resource Protection.

SEE *Archeology and Artifacts, Protection of during War.*

---

## Customs Service, United States

---

■ JUDSON KNIGHT

One of the oldest bureaus of the federal government, the United States Customs Service was founded in the first year of George Washington's presidency, and for decades the tariffs it collected funded virtually all government activities. Today, Customs is a vast border security force that yearly interdicts hundreds of millions of dollars' worth of illegal goods. Following the terrorist attacks of September 11, 2001, Customs became a significant component in homeland security operations, and in March, 2003, it moved from the Department of the Treasury to the newly created Department of Homeland Security (DHS). Among the post-September, 2001, measures it has adopted is a port security program that requires shippers to provide advance notification of cargo arriving on American shores.

### Background

Soon after Washington took office as the nation's first president, Congress passed the Tariff Act, which Washington signed on July 4, 1789. Four weeks later, on July 31—in only the fifth act of congressional history—Customs was established to protect American ports of entry. Newspapers of the day called the Tariff Act the “second Declaration of Independence,” an appellation based on something more than the date on which the act was signed: for the next 125 years, the revenue provided by import tariffs funded nearly the entire federal government.

Over the course of its long existence, Customs has administered programs that eventually passed to other departments. These included the supervision of revenue cutters, ships that patrolled the coastline—a service that ultimately became the U.S. Guard. Additionally, Customs collected hospital dues to assist sick and disabled seamen, a program now handled by the Public Health Service; collected import and export statistics before the Bureau of the Census was founded to undertake this responsibility; established standard weights and measures prior to the founding of the now-defunct National Bureau of Standards (now the National Institute of Standards and Technology); and administered military pensions many decades before the founding of the Department of Veterans Affairs.

**Customs activities.** Customs is responsible for ensuring that all imports and exports comply with U.S. laws and regulations; collecting and protecting revenue; and guarding against smuggling. Its specific duties include assessing and collecting duties, excise taxes, and penalties on imported goods; interdicting and seizing illegal items; processing persons, baggage, cargo, and mail; administering certain navigation laws; detecting and apprehending persons engaged in activities designed to circumvent Customs regulations; protecting American industry, as well as intellectual property rights, by enforcing laws to prevent illegal trade practices; enforcing import and export restrictions on dangerous items; and collecting import and export data for the compilation of international trade statistics. In addition to enforcing its own laws, Customs enforces some 400 other laws on behalf of more than 40 government agencies.

In fiscal year 2002, Customs processed some 415 million passengers and pedestrians entering or leaving U.S. territory. Additionally, it processed a total of 130 million boats, ships, passenger vehicles, trucks, buses, and aircraft, both private and commercial. In the course of these efforts, it arrested nearly 13,000 people and seized a wide array of contraband, including \$204 million in illicit proceeds, \$60 million in counterfeit goods, and \$1.3 million in merchandise; almost 4 million pounds (1.8 million kg) of marijuana, nearly 168,000 pounds (76,200 kg) of cocaine, over 4,000 pounds (1,814 kg) of heroin, 7.5 million tablets of ecstasy, and more than 3,000 pounds (1,361 kg) of methamphetamine; as well as nearly 40,000 firearms and 6.4 million rounds of ammunition.

### Protecting Homeland Security

With a mission that already made it alert to the protection of U.S. borders and ports, Customs was a key component of homeland security even before the phrase gained widespread currency in the wake of the 2001 terrorist attacks. Following those attacks, Customs undertook new measures designed to tighten points of entry and protect the borders against suspicious persons and items.

One such measure was Operation Green Quest, in which Customs teamed with multiple federal agencies to target systems used by terrorist organizations to acquire and transfer funds. Established on October 25, 2001, Operation Green Quest issued 177 search warrants, and made 79 arrests and 70 indictments within a little more than a year. The program also netted \$33 million in terrorist funds, some \$21 million of it in the form of currency and monetary instruments seized as part of the Operation Green Quest bulk cash initiative.

On December 4, 2001, Customs partnered with U.S. industry in Project Shield America, established for the purpose of protecting against the acquisition and exploitation of technological products by terrorists and terror-sponsoring nations. (Among the latter, the federal government has identified seven governments: Cuba, Iran, Iraq,



A supervisor with the Bosnia-Herzegovina State Border Service Agency uses a fiberscope to examine the gastank of a pickup truck during the International Border Interdiction Training conducted by the U.S. Customs Service at the Hidalgo port of entry in Hidalgo, Texas. AP/WIDE WORLD PHOTOS.

Libya, North Korea, Syria, and Sudan.) Of specific interest are U.S. munitions list items, and strategic dual-use technology.

**Challenges.** Post-September 2001 security measures also include several programs requiring advance notice of shipments. Through its Container Security Initiative, Customs places personnel at major foreign ports to pre-screen cargo bound for the United States. The 24-Hour Ruling, instituted in December, 2002, requires ocean carriers bringing goods to the United States to provide manifest information at least 24 hours prior to taking on cargo at the foreign port.

Additionally, in January 2003, Customs proposed new restrictions whereby it would receive four hours' advance electronic notification before imports are loaded into a truck. According to a report in *Transport Topics*, a number of truckers and shippers complained that this measure would cripple business, and one industry executive predicted that "These regulations will essentially eliminate same-day and next-day shipping." Similar restrictions

imposed on deliveries by air and rail provoked protests from a wide array of shipping-related companies.

Disagreements with shippers may not be the only challenges Customs faces in its intensified mission of homeland security. By 2003, the service ran the danger of being overtaxed, with numerous activities across a broad spectrum, including counter-narcotics programs, new border security initiatives, financial investigations, and even child pornography stings. Additionally, in January, 2003, Customs deployed two Blackhawk helicopters and two Cessna Citation jets equipped with sensors to conduct 24-hour-a-day patrols over the skies of Washington, D.C., replacing military jets that had performed that role since September, 2001.

Further complicating the picture for Customs was its transition to DHS, which would require the separation of its border inspectors from its investigators under two different branches of the new department. As of March, 2003, as DHS began operations, Customs operatives faced the problem of developing a suitable technological interface with the department, and with each other.

## ■ FURTHER READING:

### PERIODICALS:

Johnson, Jeff. "Truckers, Shippers Blast Customs Security Plan." *Transport Topics* no. 3521 (January 27, 2003): 1.

Mintz, John, and Spencer Hsu. "Customs Takes over Monitoring Local Skies." *Washington Post*. (January 28, 2003): A6.

Skrzycki, Cindy. "Security in Mind, Customs Says Cargo Can Wait." *Washington Post*. (February 11, 2003): E1.

Weiner, Tim. "Along Borders, Tension and Uncertainty Prevail." *New York Times*. (March 1, 2003): A11.

### ELECTRONIC:

U.S. Customs Service. <<http://www.customs.ustras.gov/>> (March 29, 2003).

### SEE ALSO

*Homeland Security, United States Department*  
*IBIS (Interagency Border Inspection System)*  
*Treasury Department, United States*

---

## Cyanide

---

### ■ JUDSON KNIGHT

The prospects for an intelligence operative captured by enemy forces are grim. Soldiers and other war fighters have recourse to Geneva Convention protocols concerning treatment, but personnel working in intelligence and covert operations are effectively denied such protection by virtue of their mission's clandestine nature. The best hope is to be released in a prisoner exchange, sometimes after years. Even then, imprisonment in many countries is likely to include lengthy and exposure to coercive methods, including beatings and/or torture whose intention is to induce the operative to divulge sensitive information. For some, the risk is too great, and therefore, intelligence operatives and agents have often gone into dangerous situations equipped with suicide devices. Most of these employ one form of disguise or another to hide a deadly compound of nitrogen, carbon, and other elements known as cyanide.

**The chemistry and biological effects of cyanide.** When an atom of carbon bonds with an atom of nitrogen, that is cyanide, an ionic compound designated as CN—hence the name cyanide. The bonding of these atoms with other elements produces various forms: hydrogen cyanide (HCN), cyanogen chloride (CNCl), sodium cyanide (NaCN), or potassium cyanide (KCN). The first two are colorless gases, while the second two appear in crystal form. In addition to these chemical formulas, cyanide is sometimes referred to by military organizations as AN (hydrogen cyanide) or CK (cyanogen chloride).

Applied in materials for exterminating rats and other pests, removing artificial nails, or developing photographs, cyanide has a number of practical uses. It is found in some foods, most notably cassava, and when combined with another chemical, it produces a life-sustaining substance, vitamin B<sup>12</sup>. Yet even in small quantities, cyanide is harmful, a fact illustrated by poisoning deaths in parts of Africa where the diet is heavy in cassava. Cyanide is also one of the most dangerous toxins in cigarette smoke, which is the form of cyanide to which the average person is most likely to be exposed.

Cyanide prevents the body's cells from receiving oxygen, and particularly effects the heart and brain because those two vital organs are particularly dependent on the body's oxygen supply. Within minutes, the victim of cyanide poisoning in very small quantities will begin breathing rapidly and display signs of restlessness. Other symptoms include dizziness, weakness, headache, nausea and vomiting, and a rapid heart rate. Exposure to larger amounts causes rapid convulsions, severe lowering of blood pressure and heart rate, loss of consciousness, lung injury, and ultimately respiratory failure that leads to death.

**Cyanide in history.** Because cyanide is an effective killer, Iraqi dictator Saddam Hussein included hydrogen cyanide among the chemical weapons he used against the Kurds in the Iran-Iraq war of the 1980s. Forty years earlier, during World War II, Nazi Germany used hydrogen cyanide—in the form of Zyklon B—as an even more efficient agent of genocide in its death camps, where it killed millions of Jews and others. Ironically, in the same war, the Nazis' enemies carried cyanide pills on their persons for a very different reason, to eliminate themselves if captured.

Personnel working for the Special Operations Executive (SOE) in the war were often equipped with "L" pills (*L* for *lethal*) containing cyanide in crystal form. In some cases, cyanide could be hidden in the earpiece of a pair of glasses. When cornered, the operative could take off his glasses and pretend to thoughtfully bite the end of the earpiece while thinking about what he would say next. But there would not be any next statement: within seconds of consuming this deadly toxin, the operative would be dead.

A similar situation happened in 1977, when Soviet diplomat Aleksandr Ogorodnik found that he had reached the end of the line. He had been secretly working for the U.S. Central Intelligence Agency, who knew him by the code name TRIGON. When the Soviets discovered they had a traitor in their midst, they presented him with a confession to sign. Ogorodnik, well aware of what lay in store for him, asked to use his own pen, and when it was given to him, he bit off the end, ingesting a dose of cyanide hidden there. Within seconds, he was dead.

In order to keep this means of escape handy, operatives have gone to extraordinary lengths. Among the items used for concealing cyanide pills in the past is a container shaped like a cigarette lighter and made to fit in the rectum. In 1960, U-2 pilot Francis Gary Powers carried a

cyanide capsule on his person. Instead of committing suicide, when the Soviets shot down his plane, Powers parachuted to earth, and was taken prisoner. Later, after his captors had reaped enormous propaganda benefits from the incident, he was traded for a Soviet spy in a prisoner exchange.

#### ■ FURTHER READING:

##### BOOKS:

Melton, H. Keith. *The Ultimate Spy Book*. New York: DK Publishing, 1996.

Minnery, John. *CIA Catalog of Clandestine Weapons, Tools, and Gadgets*. Boulder, CO: Paladin Press, 1990.

##### ELECTRONIC:

Facts About Suicide. Centers for Disease Control. <<http://www.bt.cdc.gov/agent/cyanide/index.asp>> (March 19, 2003).

International Spy Museum. <<http://www.spymuseum.org>> (March 19, 2003).

##### SEE ALSO

*Assassination*  
*Assassination Weapons, Mechanical*  
*Biochemical Assassination Weapons*  
*Chemical Warfare*  
*Intelligence Agent*  
*U-2 Incident*

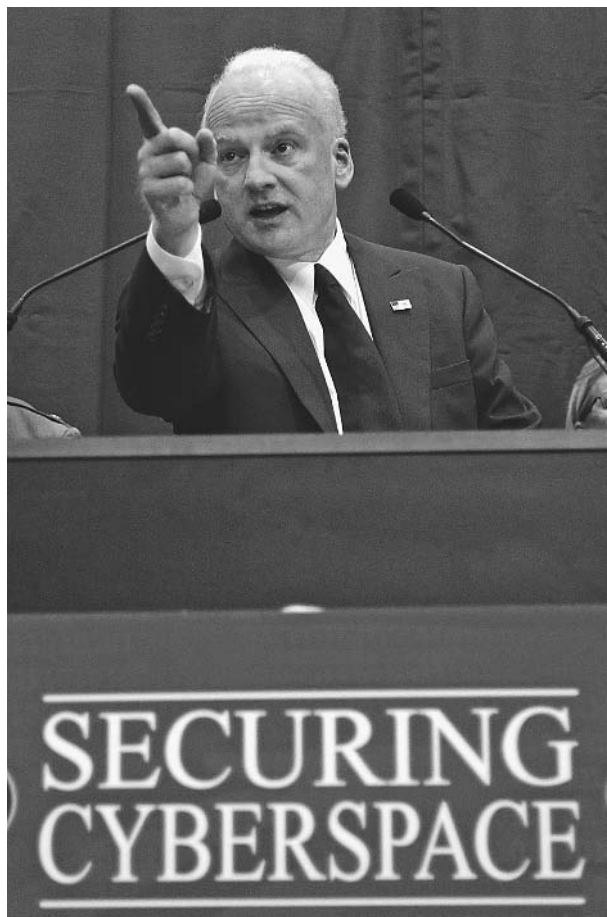
## Cyber Security

#### ■ BRIAN HOYLE

Cyber security—measures taken to protect computers and computer networks from accidental or malicious harm—is an ongoing process. The security of a system is only as strong as its weakest link. When a fault is identified and corrected, the system tends to be stronger. This state is often transient, as other faults are eventually be detected and exploited.

The very nature of the Internet makes cyberspace vulnerable to attack. The vast majority of computers connected to the Internet are IBM compatible, as are the few operating systems that control their function. An attacker who can find a security flaw in even one computer could gain access to many computers that are not protected from intrusion.

An attack can be circuitous, involving many computers. Some computers are used surreptitiously in the attack; thus, the source of an attack becomes difficult to trace, especially if the attack has disguised the source



Richard Clarke, the White House's senior security advisor, outlines the administration's 2002 cyberspace security recommendations that include educating users and urging market forces, not government mandates, to fix cybersecurity problems. AP/WIDE WORLD PHOTOS.

address. While in the past, most breaches of computer security were mischief caused by computer hackers, increasingly, the information contained within computer databanks is probed and in some cases, altered.

Such disabling of computer networks can be crippling to business or infrastructure. The 1997 Presidential Commission on Critical Infrastructure concluded that cyber security was as essential to the functioning of the United States as water supplies, and declared cyber security vital to U.S. national interests. In November 2002, the U.S. government passed the Cyber Security Research and Development Act, which dedicates almost one billion dollars to the establishment of cyber security research and training centers.

### Cyber Security Threats

A practice dubbed "dumpster diving" involves routing through the trash to recover paperwork or even used computer components that have been discarded. Even in

the computer age, many people print information and then discard it. A diligent search of a person's trash can sometimes obtain a great deal of sensitive information.

Intelligence personnel masquerading as janitors or other staff can gain access to computers in off-hours, and, utilizing deciphered user names and passwords, can delve into databases for information.

Cyber security also focuses on equipment. Computers that are linked via electrical wire (i.e., Ethernet networks) typically have many wall jacks ("network drops"), by which computers are connected to the network. A vacant network drop that has not been disabled can be surreptitiously used to connect with the network. Software is available that enables the connected computer to capture all data that is flowing through the network.

Wireless networks carry other security risks, as a rogue computer does not need to be physically connected to a network drop in order to acquire information. Furthermore, if the signal from a wireless network extends beyond the boundaries of a building, intelligence can be gathered even from someone parked outside.

Username and passwords are another vulnerable aspect of a computer network. The tendency of people to trust someone making a request for user information, and to use the same easy-to-decipher identifiers repeatedly can allow an intruder to gain access to a network.

Email is especially prone to breaches in security. The information in most emails, including the username, is in plain text. Applications are available (i.e., MailSnarf) that allow email transiting from sender to receiver to be retrieved and read by a third party. Thus, an attacker can read sensitive information contained in an email and as well, can hijack an email account to send and receive messages. Emails often have documents attached to them. This route is used to deliver malicious codes (i.e., viruses, worms, Trojan Horses) to computers.

Viruses are small programs that become embedded in files. Once a file is infected, the virus can execute its function. Depending on the intent of the virus designer, the result can be merely inconvenient to extremely destructive. Thousands of viruses exist, with new ones appearing daily. Thus, viral cyber security requires constant updating of viral protection software.

Trojan Horses are applications that are disguised as useful programs. Once activated, Trojan Horses permit a remote user to have access to the host computer, via the activated program. This aspect is especially relevant in espionage and the subterfuge can be difficult to detect.

Attackers sometimes utilize authorized network connections, in effect assuming the identity of the authorized user. Another attack strategy is called man-in-the-middle. Here, a third party—the attacker or intelligence-gatherer—impersonates both ends of a connection. The real sender and receiver are unaware that their communications are not proceeding directly to the destination. A third strategy

is called the replay attack. In the replay attack, transmissions are intercepted, read, and passed along to the rightful final destination.

## Cyber security Measures

The perimeter security model is the most popular type of cyber security model. The defenses are set to prevent intrusion while allowing authorized user activities to proceed unimpeded.

Typical perimeter defenses include firewalls (which filter incoming information according to set criteria for acceptance, such as IP address, domain name, protocol of sender-receiver communication, key words or phrases), intrusion detection systems, and virtual private network servers (where data is encrypted at the sending end and decrypted at the receiving end). When all the components are operating properly, a perimeter defense allows only those authorized activities to proceed from the 'outside' (i.e., the Internet) to the individual computer or computer network. However, improperly configured perimeter devices can create an illusion of security while offering little security at all.

**Administrative scrutiny.** Data are often backed up onto tapes. Being portable, the tapes are liable to theft. If the tape data are not encrypted, the information can be transferred or copied to another computer.

Another aspect of cyber security is the identification and approval of all hardware. The unapproved installation of a piece of hardware such as a modem or a firewall can compromise an entire network, if the installed item is not properly configured. For example, an improperly configured firewall can allow access to the Internet when only receipt and transmission of email should be permitted. A dedicated systems administrator is the best guarantee of daily scrutiny of a network's performance and vulnerability. A key component of a cyber security plan is the presence of a fallback plan in case of misadventure or deliberate sabotage.

Evaluation of the performance of some security measures is a prudent precaution. This can only be accomplished by triggering the measures by a staged attack. For example, former computer hackers are now employed by companies and government agencies to probe the vulnerabilities of a computer system. This surreptitious testing, even of the security personnel, is known as red-teaming.

**Breaching of cyber security.** Computer and network security tends to be expensive and can require additional operations on the part of the user. The installation of safeguards does not increase the operational efficiency of a computer

system, and can often add more layers to the operation of the computers. Until an attack, the value of the cyber security will be invisible. Thus, users and administrators can resist the implementation of cyber security measures. Without dedicated scrutiny, the cyber security measures that are in place can lapse over time, creating opportunities for breaching of the system.

#### ■ FURTHER READING:

##### BOOKS:

Bosworth, Seymour (ed.) and Michel E. Kabay. *Computer Security Handbook*. New York: John Wiley & Sons, 2002.

National Research Council, Computer Science and Telecommunications Board. *Cyber Security Today and Tomorrow: Pay Now or Pay Later*. Washington, DC: The National Academies Press, 2002.

Northcutt, Stephen, Lenny Zeltser, Scott Winters, et al. *Inside Network Perimeter Security: The Definitive Guide to Firewalls, Virtual Private Networks (VPNs) Routers, and Intrusion Detection Systems*. Indianapolis: New Riders Publishing, 2002.

##### ELECTRONIC:

How Stuff Works. "How Firewalls Work." Jeff Tyson. <<http://www.howstuffworks.com/firewall.htm>> (15 December 2002).

##### SEE ALSO

*Codes and Ciphers*  
*Electromagnetic Pulse*  
*Internet Spider*

---

## Cyber Security Warning Network

---

#### ■ JOSEPH PATTERSON HYDER

Communication is critical during a time of national crisis. Emergency personnel need the ability to communicate quickly and effectively with their colleagues in other parts of the country. In wartime, generals must remain in close contact with commanders and troops in the field. In the computer age, all communications systems—telephones, cellular phones, email, and others—are intertwined. A cyberattack that takes down the Internet by attacking root servers would also have a profound effect on all forms of communications, which rely on switches and routers to relay signals. Therefore, a cyberattack coordinated with other terrorist attacks or occurring during wartime could

have catastrophic effects on national security and the economy.

In 2001, the George W. Bush administration and emergency response officials began studying what would have happened if an attack on America's communication infrastructure had coincided with the September 11, 2001 terrorist attacks. The more important question, however, was how to stop such an attack. The result was the Cyber Warning Information Network (CWIN), part of Bush's National Strategy to Secure Cyberspace.

Although the CWIN is not fully operational as of 2003, one proposed function of the CWIN is to prevent cyberattacks. The CWIN will accomplish this by creating several industry specific workgroups, or Information Sharing and Analysis Centers (ISACs). Each ISAC will monitor Internet activity and cyberattacks on Web sites and Internet infrastructure within its sector. The government agencies, companies, and network security firms involved in that ISAC will then communicate with each other on cyberattacks and increase security to prevent future attacks. If action is taken quickly enough, an ISAC will be able to stop the spread of computer viruses before they strike important systems.

The Clinton administration developed the ISAC concept. Currently, ISACs exist for each of the following sectors: information technology, banking and finance, telecommunications, chemical, and energy. The Bush administration worked with government agencies and the private sector to develop ISACs for public transportation infrastructure, water treatment, and agriculture and food.

While the idea of sharing information about particular network security vulnerabilities in order to increase security for all interested parties was considered favorable, many private sector members have been slow to volunteer network and software security problems. The Freedom of Information Act covers the CWIN, so these organizations have shown hesitancy that any information shared with fellow ISAC members might become public. Until these companies receive a privacy guarantee from the government, CWIN will not function as effectively as intended.

The second major function of the CWIN will be to allow each ISAC to operate as an individual network, even if the entire Internet is damaged in a cyberattack. This will allow ISAC members to continue to exchange critical information if all other communications systems are down. The CWIN will accomplish this by establishing an independent IP network for each ISAC.

Critics have found flaws with the CWIN on both conceptual and organizational grounds. Detractors argue that in order for the CWIN to be effective, the private sector and network security professionals will have to play a major role. So far, the government has offered few incentives for the private sector to invest the money and labor necessary to accomplish this objective. The Department of Homeland Security has also concerned some of the private



sector with a lack of commitment to the CWIN. Even after the unveiling of Bush's National Strategy to Secure Cyberspace program, which includes the CWIN, the DHS had not named a person to head the CWIN.

#### ■ FURTHER READING:

##### ELECTRONIC:

MacMillan, Robert. "U.S. Heightens Cybersecurity Monitoring." *washingtonpost.com* <<http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A46583-2003Mar18-Found=true>> (18 March 2003).

##### SEE ALSO

*Computer Fraud and Abuse Act of 1986*  
*Computer Hackers*  
*Computer Software Security*  
*Computer Virus*  
*Cyber Security*  
*National Information Infrastructure Protection Act, United States*

## Czech Republic, Intelligence and Security

■ TIMOTHY G. BORDEN

Like all of the socialist governments of Eastern Europe, the Czechoslovakian regime used its intelligence and security services to clamp down on political dissent from the time it eliminated its opposition in 1948, until it was finally deposed in 1989. Although the scope and tactics of the Czech Statni Bezpecnost (StB) never reached the extent of its secret-police counterparts in East Germany or Romania, political repression was a feature of daily life in the country for its citizens. After the socialist regime fell in the peaceful Velvet Revolution of late 1989, the new, democratic government moved quickly to reorganize its security and intelligence operations and implemented a novel program to purge former high-level collaborators with the StB from retaining their public posts.

After assuming power in disputed elections in 1948, the Czechoslovakian Communist Party ruled the nation as a satellite of the Soviet Union. Its foreign and domestic policies closely followed that of its dominant partner and the Czechoslovak regime consistently passed intelligence information to the KGB. The brief period of reform in the Czechoslovakian Communist Party under Alexander Dubcek (1921–1992), known as the Prague Spring, came to an abrupt end with the Soviet-led Warsaw Pact invasion of

August 1968. The government reverted to its former repression and maintained a network of informants working for the Statni Bezpecnost (StB), or secret police, which had its own staff of about 17,000 agents. The operatives were active in reporting and suppressing dissent among religious, academic, and political groups. The regime also maintained a higher standard of living compared to other Soviet-bloc nations, which further helped to diminish political opposition. The combination of repression and material incentives succeeded in stifling the once-restive Czechoslovakian people through the 1970s and well into the 1980s.

Domestic reform movements overturned the socialist regime with surprising swiftness and nonviolence during the Velvet Revolution of late 1989, when dissident writer Vaclav Havel emerged as the nation's president. In 1992, Havel also presided over the separation of Czechoslovakia into the independent entities of the Czech Republic and Slovakia. The government of the new Czech Republic maintained the four intelligence agencies that were established in May 1991. Two of the agencies, the Czech Security Information Service (Bezpecnostni Informacni Sluzba, or BIS) and Office for Foreign Relations and Information (Urad pro Zahranicni Styky a Informace, or USZI), gathered domestic and international information related to the protection of democracy, national interests, and human rights. The other two agencies, the Intelligence Service of the General Staff (Zpravodajska Sprava Generalniko Stab, or ZSGS) and the Military Defense Intelligence Agency, gathered information related to military interests. In contrast to the StB, the new civilian agencies did not retain executive powers of arrest and detention and were pledged to maintain the Constitutional rights of every citizen. The agencies also faced the challenge of training their new personnel in intelligence technology and surveillance and enlisted the aid of the United States, Great Britain, and the Netherlands in providing technical training in the 1990s.

Another major task of the new democratic government was implementing the lustration law passed in October 1991. Under the lustration process those who were found to have collaborated with the secret police during socialist rule were barred from a number of public posts, including the state's judicial system, central bank, and other high-level civil service, military, and academic posts. Through the expiration of the law at the end of 2000, over 300,000 lustration investigations took place under the Civic Forum, an independent commission. Less than five percent of the cases resulted in findings of collaboration with the StB and ultimately only about one hundred people were barred from their positions at the conclusion of their hearings. Other European countries adopted similar lustration laws during their transitions to democracy, including Hungary, Bulgaria, and Poland. The process went the furthest in the former German Democratic Republic (East Germany), where the Gauck Authority disseminated information from the Ministry for State Security (or Stasi) files.



During a 2002 ceremony, former Czech President Vaclav Havel, right, presents Vice Admiral Thomas R. Wilson, director of the U.S. Defense Intelligence Agency (DIA), with the Order of the White Lion for his contributions to Czech defense and intelligence in Prague. AP/WIDE WORLD PHOTOS.

#### ■ FURTHER READING:

##### BOOKS:

Ulrich, Marybeth P. *Democratizing Communist Militaries: The Cases of the Czech and Russian Armed Forces*. Ann Arbor: University of Michigan Press, 2000.

Williams, Kieran and Dennis Deletant. *Security Intelligence Services in New Democracies: The Czech Republic, Slovakia, and Romania*. New York: Palgrave Macmillan, 2001.

##### ELECTRONIC:

Central Europe Review. "A Scorecard for Czech Lustration." Kieran Williams. November 1, 1999. <<http://www.ce-review.org/99/19/williams19.html>> (March 6, 2003).

Czech Security Information Service. "Intelligence Means." <[http://www.bis.cz/eng/a\\_prostredky.html](http://www.bis.cz/eng/a_prostredky.html)> (March 6, 2003).

———. "Terrorism, Extremism, and Organised Crime." <[http://www.bis.cz/eng/a\\_ismy.html](http://www.bis.cz/eng/a_ismy.html)> (March 6, 2003).

Federation of American Scientists. "Czech Republic: Intelligence." John Pike. January 5, 2003. <<http://www.fas.org/irp/world/czech/>> (March 6, 2003).

##### SEE ALSO

*Cold War (1945–1950), The Start of the Atomic Age*

*Cold War (1950–1972)*

*Cold War (1972–1989): The Collapse of the Soviet Union*

*Intelligence and Democracy: Issues and Conflicts*

*Slovakia, Intelligence and Security*

*Soviet Union (USSR), Intelligence and Security*

*STASI*

*This page intentionally left blank*



---

## D Notice

---

■ ADRIENNE WILMOTH LERNER

D Notice (defense notice) refers to an alert given by intelligence services or the armed forces to the media, alerting them of sensitive content that could damage national security or defense if reported in part or in whole. In Britain, the system is somewhat voluntary and various media corporations are not obliged to report or refrain from reporting, potentially sensitive issues.

The British D Notice system, the first of its kind, was established in 1912. Later the process was bolstered by the passage of the Official Secrets Act, which defined subjects that are not cleared for public broadcast. The act was intended to prevent information from falling into enemy hands. The notices then pertained to wire transfers, and have since evolved with the progression of technology. Today, D Notices cover media broadcast content via radio, films, television, and the Internet.

The parameters for information requiring a D Notice are straightforward. Defense plans, specific training regimens, and vital troop readiness statistics are discouraged from being broadcast. Reports on the specific operation of intelligence services, defense equipment, ciphers and data security systems are flagged for D Notices, as is the subject of civil defense, and nuclear weapons equipment and testing. The specificity and nature of a given journalistic piece, as well as the time and circumstance during which the report is broadcast, are all considered in the D Notice process. Perhaps the largest factor in the process is what type of media will be airing the piece. Television and film cameras, as well as still photographs, can often reveal more than words alone.

D Notices have again reentered the public consciousness, and are often called DA Notices (defense advisory notices). During the Persian Gulf War, several government and military officials from various nations complained

that intense media coverage let Iraq prepare for every American strike. In late 2002, a new rash of D Notices were issued for information coming from military operations in the Middle East. Some journalists hold that D Notices are too often issued for subjects that are merely unflattering to government, rather than a matter of national defense, and thus are a form of soft censorship. On the whole, media companies and individual journalists are increasingly opting out of cooperating with D Notices advisories, when possible. However, there is always the possibility of professional disciplinary action, or legal punishment, such as suspension of broadcasting privileges or a steep fine, for refusal to heed some especially sensitive D Notice warnings.

### ■ FURTHER READING:

#### ELECTRONIC:

Wilkins, Gus. "The DA-Notice Web site-The Official Site of the Defence, Press and Broadcasting Advisory Committee." <<http://www.dnotice.org.uk/index.htm>> (December 1, 2002).

---

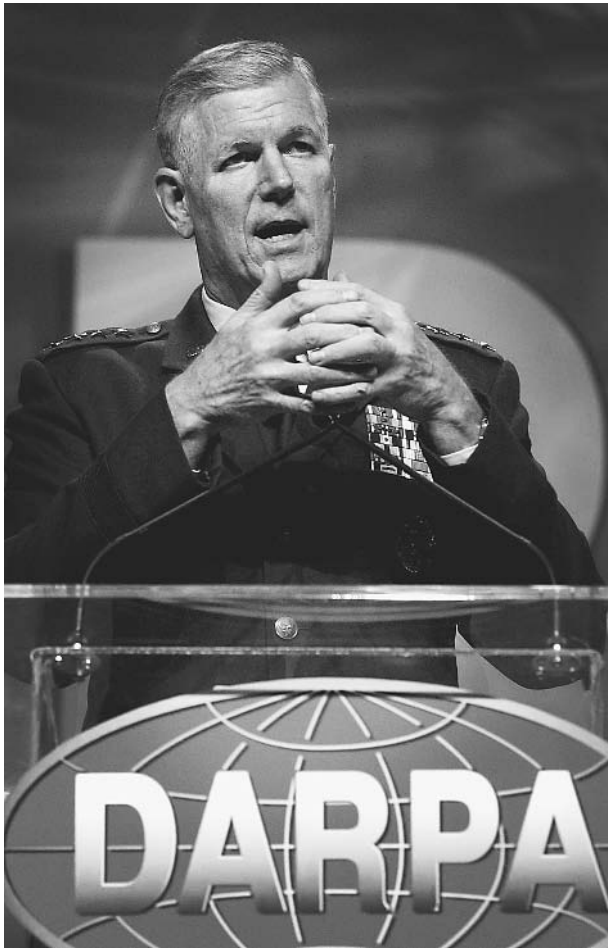
## DARPA (Defense Advanced Research Projects Agency)

---

■ K. LEE LERNER

The Defense Advanced Research Projects Agency (DARPA) is the central United States Department of Defense agency dedicated to advancing research in areas of science and technology that may directly enhance military effectiveness.

DARPA's development of the TCP/IP network protocol architecture and packet switching and significantly



Air Force General Richard B. Myers, chairman of the Joint Chiefs of Staff, stresses the need for the different branches of the military, as well as the providers of weapons and technology, to work as a cohesive unit at a 2002 conference of the Defense Advanced Research Projects Agency (DARPA). AP/WIDE WORLD PHOTOS.

contributed to the development of the Internet during the 1960s-1970s (then known as ARPANet).

The launch of The Soviet satellite *Sputnik* in 1958 fueled the creation of DARPA. Eventually DARPA's programs related to utilization of space were transferred over to the National Aeronautics and Space Administration (NASA) or the National Reconnaissance Office (NRO). Currently, DARPA continues research in space programs related to rapid use of the near space environment. DARPAS space use programs include the Responsive Access, Small Cargo, Affordable Launch (RASCAL) program, Orbital Express program, and the Space Surveillance Telescope (SST) capable of detecting small satellites and other military hardware placed in geosynchronous orbit.

During the Cold War, DARPA placed emphasis on developing technology related to ballistic missile defense. In 1968, DARPA programs became the foundation for the Army Ballistic Missile Defense Agency (ABMDA).

DARPA is specifically charged to maintain the technological superiority of U.S. military forces. Instead of funding projects based upon traditional criteria (i.e., expectations of anticipated results), DARPA strives for innovation in technology—including areas and projects with a low probability of success. This approach does not allow the direct development of technology but helps to prevent technological surprise by potential enemies.

As much as a governmental agency is able, DARPA has embraced an entrepreneurial oversight approach that facilitates rapid project start-up and strives to keep projects from becoming entrenched in traditional research funding mires. In some cases, DARPA can operate outside of traditional Civil Service rules and procure material support for projects outside of Federal regulations related to funding, bidding, and acquisition.

DARPA does not directly operate laboratories or facilities. DARPA is organized around a technology branch—a branch that encompasses DARPA's Defense Sciences Office, Information Processing Technology Office, and the Microsystems Technology Office—and system branch encompassing DARPA's Tactical Technology Office, Advanced Technology Office, Information Exploitation Office, Special Projects Office, and Information Awareness Office.

DARPA also encourages research by offering and awarding monetary prizes. For example, DARPA decided to offer a substantial monetary prize to the winner of a race of fully autonomous, unmanned ground vehicles from Los Angeles to Las Vegas set for April 2004. For the Army and Marines, DARPA's project AGILE led to the development of the modern M-16 rifle.

DARPA's HAVE BLUE and TACIT BLUE programs led to the development of the F-117 stealth fighter and B-2 stealth bomber used by the U.S. Air Force. Current DARPA programs seek to advance hypersonic flight capabilities. DARPA stealth programs include the SEA SHADOW program designed to apply stealth technology to naval vessels.

As of 2003, DARPA emphasized research in counterterrorism, assured use of the near space environment, networked manned and unmanned systems, self-forming robust networks, technologies to detect and destroy elusive surface targets; remote sensing and characterization of underground structures, biotechnology, and cognitive computing capabilities (i.e., computing systems that have the ability to reason and learn).

#### ■ FURTHER READING:

##### ELECTRONIC:

DARPA Offices and programs. May, 2003. <[www.DARPA.mil](http://www.DARPA.mil)> (May 10, 2003).

##### SEE ALSO

*Biological and Biomimetic Systems*  
*Biological Input/Output Systems (BIOS)*

*Biological Warfare, Advanced Diagnostics*  
*Bio-Magnetics*  
*Bio-Optic Synthetic Systems (BOSS)*  
*Bioshield Project*  
*Bioterrorism*  
*Brain-Machine Interfaces*  
*Molecular Biology: Applications to Espionage, Intelligence and Security*  
*Nanotechnology*  
*NSF (National Science Foundation)*  
*Pathogen Genomic Sequencing*  
*Quantum Physics: Applications to Espionage, Intelligence, and Security Issues*  
*Robotic vehicles*  
*Tissue-Based Biosensors*  
*Unmanned Aerial Vehicles (UAVs)*

## Data Mining

■ BRIAN HOYLE

Data mining refers to the statistical analysis techniques used to search through large amounts of data to discover trends or patterns.

Data mining is an especially powerful tool in the examination and analysis of huge databases. With the advent of the Internet, vast amounts of data are accumulating. As well, the amount of data that can be generated from a single scientific experiment where stretches of DNA are affixed to a glass chip can be staggering. Visual inspection of the data is no longer sufficient to make a meaningful interpretation of the information. Computer-driven solutions are required. For example, to analyze the DNA chip data, the discipline of bioinformatics—essentially a data mining exercise—emerged in the 1990s as a powerful melding of biology and computer science.

The collection of intelligence and the monitoring of the activities of a government or an organization also involves sifting through great amounts of data. Coded information can be inserted into data transmissions. If this information escapes detection, it can be used for undesirable purposes. The ability to extract the suspect information from the background of the other information is of tremendous benefit to security and intelligence agencies.

An example of data mining that is of relevance to espionage, intelligence and security is the use of computer programs—such as the Carnivore program of the United States Federal Bureau of Investigation—to screen thousands of email messages or Web pages for suspicious or incriminating data. Another example is the screening of radio transmissions and television broadcasts for codes.

The formulas used in data mining are known as algorithms. Two common data mining algorithms are

regression analysis and classification analysis. Regression analysis is used with numerical data (quantitative data). This analysis constructs a mathematical formula that describes the pattern of the data. The formula can be used to predict future behavior of data, and so is known as the predictive model of data mining.

For example, from a database of terrorists who have corresponded using emails, predictions could be made as to who will send an email and to whom. This would aid efforts to intercept the transmission. This type of data mining is also referred to as text mining.

Data that is not numerical (i.e., colors, names, opinions) is called qualitative data. To analyze this information, classification analysis is best. This model of data mining is also known as the descriptive model.

The data mining process involves several steps:

- Defining the problem.
- Building the database.
- Examining the data.
- Preparing a model to be used to probe the data.
- Testing the model.
- Using the model.
- Putting the results into action.

Database construction and model preparation—in essence the building of the framework for the mining exercise—requires about 90% of the data mining effort. If these fundamentals are done correctly, the use of the model will uncover the data that is of potential significance.

In July 2002, the Intelligence Technology Innovation Center, which is administered by the United States Central Intelligence Agency (CIA), pledged up to \$8 million to the National Science Foundation, to bolster ongoing research into data mining techniques. United States intelligence officials suppose that terrorist organizations use Web pages and email to send encoded messages concerning future activities. Currently, unless a message is accidentally uncovered, only monitoring every Internet transmission from a region can reliably discover the covert information.

Also in 2002, the U.S. Federal Bureau of Investigation and the Central Intelligence Agency, under the direction of the Office for Homeland Security, have begun the joint development of a supercomputer data mining system. The system will create a database that can be used by federal, state, and local law enforcement agencies. Currently, the FBI and CIA have their own databases.

Another aspect of data mining is the linking together of data that resides in different databases, such as those maintained by the FBI and the CIA. Often, different databases cannot be searched by the same mechanism, as the language of computer-to-computer communication (protocol) differs from one database to another. This problem also hampers the development of bioinformatics (the computer-assisted examination of large amounts of biological



The Society of Competitive Intelligence Professionals convened in Seattle in 2001, where representatives of data-mining services such as Don Smith, shown here, gathered to exhibit new software and explain their data-mining techniques. AP/WIDE WORLD PHOTOS.

data). Increasingly, biological and computer scientists are advocating that databases be constructed using a similar template, or that they be amenable to analysis using the same search method.

#### ■ FURTHER READING:

##### BOOKS:

Edelstein, Herbert A. *Introduction to Data Mining and Knowledge Discovery*, Third Edition. Potomac, MD: Two Crows Corporation, 1999.

Han, Jiawei and Micheline Kamber. *Data Mining: Concepts and Techniques*. New York: Morgan Kaufmann Publishers, 2000.

##### ELECTRONIC:

What You Need To Know About. "Data Mining: An Introduction." About.com. <<http://databases.about.com/library/weekly/aa100700a.htm>>(17 December 2002).

##### SEE ALSO

*Cyber Security*  
*Information Security*

## DCI (Director of the Central Intelligence Agency)

#### ■ JUDSON KNIGHT

The director of Central Intelligence (DCI) is the head of the U.S. Central Intelligence Agency (CIA), principal intelligence advisor to the president, and leader of the U.S. Intelligence Community. The director oversees intelligence activities both on a broad scale, and through highly targeted operations such as the DCI Crime and Narcotics Center, the DCI Counterterrorist Center, and the DCI Center for Weapons Intelligence, Nonproliferation, and Arms Control. DCI also prepares the annual intelligence community budget, and chairs two advisory boards, the National Foreign Intelligence Board and the Intelligence Community Executive Committee. Notable DCIs of the past include Allen W. Dulles, the consummate 1950s cold warrior; Richard M. Helms, who led the CIA in the Vietnam and Watergate eras; Stansfield Turner, who sought to clean up the agency in the wake of scandals in the 1970s; and



CIA director George Tenet, right, huddles with CIA Assistant Director Dale Watson during testimony before the Senate Intelligence Committee in 2002, during which Tenet told the committee that Osama bin Laden's al-Qaeda terror group remained the most immediate threat facing the U.S. AP/WIDE WORLD PHOTOS.

William J. Casey, a key figure in the Iran-Contra affair. The list of DCIs also includes a man who went on to hold the nation's highest office: George H. W. Bush.

## Directors of Central Intelligence: 1946–73

The title of the DCI is actually older than the CIA itself: President Harry S. Truman first used it in a January 22, 1946, presidential directive, when he designated it as the lead position in the Central Intelligence Group (CIG) within the National Intelligence Authority (NIA). It was in this capacity that the first DCI, Rear Admiral Sidney W. Souers, served during his brief tenure (January 23–June 10, 1946). Lieutenant General Hoyt S. Vandenberg (June 10, 1946–May 1, 1947) also served as DCI prior to the establishment of the CIA.

The latter was created under the National Security Act of July 26, 1947, which also created the National Security Council (NSC), and it began operation on September 18. On May 1, Rear Admiral Roscoe H. Hillenkoetter became DCI, and on December 19, the NSC gave him orders for the CIA to conduct its first covert operation intended to influence the general elections in Italy so as to prevent a Communist victory. So successful was this effort that the

CIA's leadership became convinced of the efficacy of covert action.

Despite this success, Truman blamed Hillenkoetter for failing to predict the coming of the Korean War, and replaced him with General Walter Bedell Smith on October 7, 1950. Smith held the position throughout the entirety of the Korean War, and it was under his leadership that the CIA undertook one of its more notorious early covert actions by helping to bring about the overthrow of Iran's Premier Mohammed Mossadegh after the latter nationalized oil fields in his country. Smith resigned on February 9, 1953, after President Dwight D. Eisenhower—on whose staff he had served in World War II—appointed him under secretary of state.

**Dulles and the 1950s.** The accession of Allen W. Dulles to the position of DCI on February 26, 1953, marked the beginning of a new era. Whereas most of his predecessors had served in military intelligence units during the war, Dulles came from the organization of which the CIA was both a successor and an opposite: the Organization for Strategic Services (OSS). Having served as chief of OSS operations in Europe, Dulles brought expertise to the job. Dulles's grandfather, uncle, and brother all served as U.S. secretaries of state, but in contrast to his family's penchant for



diplomacy, he favored action. Under his direction, the CIA became highly energetic and enterprising, building both the Berlin Tunnel and the U-2 spy plane, and undertaking covert operations in Guatemala, Egypt, Indonesia, Chile, and the Congo.

Despite a number of successes, the CIA under Dulles also experienced several disasters, most notably the shootdown of U-2 pilot Francis Gary Powers over the Soviet Union in 1960, and the abortive invasion of Cuba at the Bay of Pigs in 1961. Though Richard Bissell, one of Dulles's lieutenants, was actually more involved with these two fiascoes, President John F. Kennedy blamed Dulles, and demanded his resignation.

**The early 1960s.** Under John A. McCone, who replaced Dulles on November 29, 1961, the CIA regained favor with Kennedy when it furnished spy plane photos showing Soviet missile emplacements in Cuba, evidence Kennedy used during the Cuban Missile Crisis.

Vice Admiral William F. Raborn, Jr. had little background in intelligence when fellow Texan Lyndon B. Johnson appointed him DCI on April 28, 1965. His lack of experience showed in his handling of the U.S. intervention in the Dominican Republic in 1965, when he passed directly to Johnson a great deal of data that had not been processed by CIA analysts. His deputy DCI (DDCI), Richard McGarrah Helms, put a stop to this indiscriminate flow of raw information, and on June 30, 1966, Helms took Raborn's place.

**Helms: mid-1960s-early 1970s.** Helms, who as DDCI had already put considerable CIA resources into the war in Vietnam, built up the CIA office in Saigon at the expense of stations around the world. He vigorously prosecuted the CIA's secret wars in Cambodia and Laos, and under his aegis the proprietary airline, Air America—actually established much earlier—flourished. Yet, for all his pragmatism, Helms maintained an idealism about intelligence work, and this would put him at odds with both Johnson and Richard M. Nixon.

First Johnson in the 1960s, then Nixon in the early 1970s, sought to involve Helms in domestic intelligence-gathering. The degree to which Helms willingly participated in these activities is a subject of some dispute, but it is clear that when Nixon sought to involve him more heavily in questionable activities, Helms objected. In particular, Nixon requested secret details involving Kennedy's debacles such as the Bay of Pigs. Nixon relieved Helms of his position on February 2, 1973.

## Directors of Central Intelligence: 1973-Present

James R. Schlesinger had the shortest tenure of any DCI: exactly five months. During that short time, he set about

revamping the agency, calling for the firing of some 1,000 employees and compiling a list of agency secrets that his successor would reveal to Congress. For two months after his July 2, 1973, departure, the DCI's position went unfilled; then, on September 4, William E. Colby took leadership. Colby's was an extremely difficult tenure, as the CIA came under intense scrutiny during this time.

In a feud with CIA counterintelligence chief James Jesus Angleton, Colby told *New York Times* reporter Seymour Hersh of a domestic intelligence campaign, Chaos, that he claimed was Angleton's brainchild. Colby did eventually relieve the CIA of Angleton, whose hunt for moles in the organization had become a preoccupation, but the revelations to Hersh set off a flurry of suspicions on Capitol Hill. During the latter part of Colby's tenure, the CIA would come under the scrutiny of multiple congressional committees, and Colby would reveal the details of the secrets compiled by Schlesinger—a list of misdeeds nicknamed "the Family Jewels".

**The late 1970s: Bush and Turner.** Colby retired on January 30, 1976, and was replaced by George H. W. Bush. Despite the overall significance of Bush's career, his tenure as DCI was short—slightly less than one year. Bush did, however, put considerable support behind intelligence-gathering technology, and the Keyhole satellite program flourished under his leadership. In the midst of ongoing debates regarding proposals to transfer the Panama Canal to Panamanian oversight, Bush learned of an effort by a Panamanian lieutenant colonel to purchase U.S. intelligence secrets. Given the volatile atmosphere surrounding the Canal transfer debate, Bush opted not to act against the colonel. Twelve years later, as president, he would unseat the Panamanian, Manuel Noriega, who by then was a general and dictator of his nation.

Bush's tenure ended on the day James E. Carter became president, as Carter had his own choice for DCI: Admiral Stansfield Turner, who took office on March 9, 1977. Although Turner was an old Naval Academy classmate of Carter, the two men barely knew one another at the time of his appointment. In contrast to the early days of CIA when DCIs tended to be military officers, Turner, who retired from active duty in December 1978, had been the only military officer to serve in the position since 1966.

Turner continued Bush's emphasis on intelligence collection via satellite, and favored electronic intelligence over human intelligence. This preference had much to do with his desire to distance the agency from its old practices, and covert operations declined dramatically under his leadership. The value of those decisions came in to question, however, when the CIA was later in a poor position to gain and analyze intelligence from human sources that could help foresee or intervene in events such as the Soviet invasion of Afghanistan or the Islamic fundamentalist takeover in Iran.

**The 1980s: Casey.** Whereas Turner was an outsider—a military man whose methods sometimes clashed with the culture of CIA—William J. Casey, who replaced him on January 28, 1981, was an old-time spy. As the last of the former OSS men—a group that also included Helms and Colby—to serve as DCI, Casey ran the agency as a fiefdom, and kept as much secret from Congress as he could.

The CIA's budget, size, and influence grew enormously under Casey, who enjoyed strong support from President Ronald Reagan. Casey reportedly directed funds and arms to rebels fighting Communist regimes in both Afghanistan and Nicaragua, and became heavily involved in the Iran-Contra affair. How great that involvement was may never be known, in part because Casey's staff deceived Congress regarding their activities, and in part because Casey died on January 29, 1987, before he could testify.

**From the mid-1980s to the present.** William H. Webster has been the only man to serve both as FBI director (1978–87) and DCI (May 26, 1987–August 31, 1991). He sought to reform the abuses that had occurred under Casey, while strengthening counterintelligence. However, the degree to which counterintelligence was strengthened would be open to question after the revelation in 1994 that the CIA had long had a highly paid Soviet mole, Aldrich Ames, in its midst.

Before becoming DCI on November 6, 1991, Robert M. Gates had already served as DDCI for many years, and even served as acting DCI during Casey's illness. As DCI (a job to which Bush appointed him), he led the redirection of CIA efforts away from their Cold War orientation, and toward a focus on issues such as nonproliferation, terrorism, and drug trafficking. During an October, 1992 visit to Moscow, Gates did something inconceivable for a DCI in Dulles's time: he entered the Kremlin.

President William J. Clinton replaced Gates with R. James Woolsey, who served two years and resigned on January 10, 1995, amid criticism concerning CIA's handling of the Ames case. John M. Deutch, who took office on May 10, 1995, became the first DCI to serve on the president's cabinet. His tenure was a short one as well, ending on December 15, 1996. During that time, however, he had put considerable effort into reform of the organization. George J. Tenet, who became the fifth DCI in just six years when he assumed leadership on July 11, 1997, set the tone for his no-nonsense style of leadership in a statement of the CIA's purpose in the post-Cold War world:

"At the end of the day, this is an espionage organization. It must generate information that is unique . . . otherwise we don't know why we are here. We no longer are in search of a mission. We know what the mission is, we know what the targets are."

The DCI serves a triple function: head of CIA, principal intelligence advisor to the president, and director of the

Intelligence Community. He reports to the president, both directly and through the national security advisor and/or the NSC, of which he is a member and intelligence advisor. DCI oversees the preparation of the annual CIA budget, which is in turn part of the Intelligence Community budget, a request he presents as a whole to the president.

DCI is also responsible for directing and coordinating national foreign intelligence activities, though he only exercises direct authority over the CIA, as well as some staff organizations outside the agency. The latter include the National Intelligence Council (NIC), which is responsible for preparing national intelligence estimates, and the Community Management Staff, which assists him in his executive functions as chief of the intelligence community. He also chairs two intelligence advisory boards, the National Foreign Intelligence Board and the Intelligence Community Executive Committee.

As head of the CIA, the DCI oversees a vast network of offices, and is involved in several offices within the directorate of intelligence that are concerned with issues that affect national security in the twenty-first century—namely, drug trafficking, terrorism, and weapons proliferation. These offices are the DCI Crime and Narcotics Center (CNC), the DCI Counterterrorist Center (CTC), and the DCI Center for Weapons Intelligence, Nonproliferation, and Arms Control (WINPAC).

Working on behalf of lawmakers and the law enforcement community, the CNC collects and analyzes information on international drug trafficking and organized crime. Its staff is made of a diverse array of personnel trained in areas ranging from international finance, to remote sensing, to foreign languages. Its strategic analysts prepare papers and briefings on both long-term trends and late-breaking events, while its targeting analysts conduct in-depth research of high-priority criminal and drug-trafficking organizations. Operating support specialists and program managers assist colleagues overseas with up-to-the-minute information on crime and narcotics issues, and remote sensing and geographic information specialists use cutting-edge technologies to detect narcotics crops and manufacturing facilities overseas.

The CTC is actually independent of the directorate of intelligence, although its Office of Terrorism Analysis (OTA) belongs to that directorate. Established by Casey in 1986 upon the recommendation of a task force chaired by then-Vice President Bush, CTC is designed to assist DCI in coordinating Intelligence Community antiterrorism efforts. OTA, its analytic component, monitors and assesses crosscutting issues and emerging trends in terrorism. Its responsibilities include tracking terrorists, analyzing worldwide terrorist threat warning information, assessing terrorist issues that cross national or regional boundaries, and producing intelligence to help interdict the flow of funds to terrorist organizations.

WINPAC provides intelligence support to U.S. policymakers the military with the aim of protecting the

United States and its interests from foreign weapons threats. Its staff includes mathematicians, engineers, physicists, economists, political scientists, chemists, biologists, and others. It studies the development of weapons across a broad spectrum, including weapons of mass destruction, advanced conventional weapons such as laser devices, and missiles. It monitors strategic arms control agreements, and supports military and diplomatic operations overseas.

#### ■ FURTHER READING:

##### BOOKS:

- Colby, William, and Peter Forbath. *Honorable Men: My Life in the CIA*. New York: Simon and Schuster, 1978.
- Grose, Peter. *Gentleman Spy: The Life of Allen Dulles*. Boston: Houghton Mifflin, 1994.
- Montague, Ludwell Lee. *General Walter Bedell Smith as Director of Central Intelligence, October 1950-February 1953*. University Park: Pennsylvania State University Press, 1992.
- Persico, Joseph E. *Casey: From the OSS to the CIA*. New York: Viking, 1990.
- Polmar, Norman, and Thomas B. Allen. *Spy Book: The Encyclopedia of Espionage*. New York: Random House, 1998.
- Powers, Thomas. *The Man who Kept the Secrets: Richard Helms and the CIA*. New York: Knopf, 1979.
- Prados, John. *Lost Crusader: The Secret Wars of CIA Director William Colby*. New York: Oxford University Press, 2003.
- Thomas, Evan. *The Very Best Men: Four Who Dared: The Early Years of the CIA*. New York: Simon & Schuster, 1995.
- Turner, Stansfield. *Secrecy and Democracy: The CIA in Transition*. Boston: Houghton Mifflin, 1985.

##### ELECTRONIC:

- Central Intelligence Agency. <<http://www.cia.gov/>> (April 24, 2003).
- Central Intelligence Agency. Federation of American Scientists. <<http://www.fas.org/irp/cia/index.html>> (April 24, 2003).

##### SEE ALSO

*Americas, Modern U.S. Security Policy and Interventions*  
*Ames (Aldrich H.) Espionage Case*  
*Bay of Pigs*  
*CIA (United States Central Intelligence Agency)*  
*CIA, Formation and History*  
*CIA, Legal Restriction*  
*Covert Operations*  
*Cuban Missile Crisis*  
*HUMINT (Human Intelligence)*  
*Intelligence, United States Congressional Oversight*  
*Intelligence Community*  
*Moles*  
*OSS (United States Office of Strategic Services)*

*Satellites, Spy*  
*U-2 Incident*  
*Vietnam War*  
*Watergate*

## DEA (Drug Enforcement Administration)

#### ■ JUDSON KNIGHT

The Drug Enforcement Administration (DEA) is the lead agency of the United States government for the enforcement of federal statutes on narcotics and controlled substances. Created in 1973, it is a division of the Department of Justice with offices throughout the United States, and in 56 countries. DEA has numerous enforcement, education, and interdiction programs, an array as varied as the range of illegal drugs and the variety of groups to which they appeal. Of particular interest within the context of espionage is DEA's intelligence function, much of which is centered at the El Paso Intelligence Center (EPIC).

### Historical Background

The genealogy of DEA involves entities, not only of the Justice Department, but also of Treasury and even the now-defunct Department of Health, Education, and Welfare (HEW). From 1915 to 1927, what traffic in illegal drugs there was in the United States was the purview of Treasury's Bureau of Internal Revenue, which in 1927 turned this responsibility over to the Bureau of Prohibition. In 1930, Treasury established the Bureau of Narcotics, the principal drug-fighting agency of the federal government for more than a generation.

When the government set out to fight illegal drugs during World War I, the use of marijuana and cocaine was a marginal activity, while some synthetic drugs, such as LSD, had yet to be invented. By the mid-1960s, however, the rising culture of psychedelia, closely tied with the antiwar movement and a generalized opposition to "the establishment," had catapulted drug use into the center of the youth culture. Recognizing these changes, HEW in 1966 established the Bureau of Drug Abuse Control within the Food and Drug Administration, and in 1968 this merged with the Bureau of Narcotics to become the Bureau of Narcotics and Dangerous Drugs, the first Justice Department incarnation of what was to become DEA.

**DEA in the 1970s and 1980s.** On July 1, 1973, the Bureau of Narcotics and Dangerous Drugs became DEA, which arrived on the scene as drug use was spreading from college



A Drug Enforcement Agency (DEA) agent stands guard next to 5,137 pounds of cocaine seized from a Panamanian vessel in Miami, Florida. AP/WIDE WORLD PHOTOS.

campuses to the mainstream of middle-class life. At no time before or since has drug use been as socially acceptable as it was in the 1970s, and DEA faced an uphill battle both culturally and operationally. The extraordinary growth in marijuana and cocaine use was coupled with a staggering rise in drug traffic from Colombia, Mexico, and other countries, and DEA greatly increased its interdiction efforts at borders, harbors, and airports.

Drug use in the United States reached an all-time high in 1979, and began to steadily decline thereafter. The change is one for which DEA rightly claims considerable credit, but a number of factors contributed. Some were at the level of policy, both public and private, including the “war of drugs” initiated by President Ronald Reagan, the “Just Say No” campaign of First Lady Nancy Reagan, and the efforts of companies who contributed airtime, advertising space, and creative talents to the Partnership for a

Drug-Free America. But a societal change was also underway, closely tied with the 1980s emphasis on traditional values, health and fitness, and self-help. By the beginning of the 1990s, Alcoholics Anonymous and other addiction recovery groups were as popular as drugs and alcohol had been a decade earlier.

**New drugs and new challenges.** Even as drug use became less widespread, the level of commitment to drugs on the part of users deepened. This was accompanied by the rise of ever more dangerous drugs. In the mid-1980s, there was ecstasy, followed by an extraordinarily lethal cocaine derivative called crack. The underpinning of new criminal enterprises, crack spawned an attendant culture in America’s inner cities, but the drug knew no ethnic barriers: users of all backgrounds joined the ranks of those addicted to this powerful narcotic.

Just as marijuana and even cocaine had once been mainstreamed among the youth culture as a whole, by the early 1990s one of the most powerful drugs of all, heroin, became a fixture among a much smaller youth segment of “Generation X.” Pundits even spoke of “heroin chic,” a gaunt look attended by a lackadaisical demeanor and unkempt clothing, which penetrated fashion and culture in general. This was followed a few years later by the surge in popularity of methamphetamines and other synthetic stimulants, produced in illegal laboratories across the nation.

**September 11, 2001, and narcoterrorism.** The September 11, 2001, terrorist attacks heightened popular awareness regarding the connection between drugs and terrorism: the Taliban, Al Qaeda’s fundamentalist Muslim hosts in Afghanistan, profited from the cultivation of poppies for making opium and heroin. But “narcoterrorism” was nothing new: for years, drug producers in Colombia, Peru, and elsewhere in Latin America had either been in league with, or even controlled by, radical or terrorist groups.

DEA analysts predicted that the connection between terrorism and drugs would only increase, inasmuch as former state sponsors of terrorism had either ceased to exist or had curtailed their activities. In the 1970s and early 1980s, Libya’s Muammar Qaddafi had been a prominent sponsor of terrorist groups from Ireland to the Philippines, while the Soviet Union had its hand either directly or indirectly in terrorist activities throughout Western Europe and other regions. Qaddafi became much less involved in terrorism after the 1986 U.S. bombing of Libya, however, and the fall of Soviet Communism cut off millions of dollars in terrorist funding. Terrorists now turned to bank robbery, kidnapping, and drug trafficking to fund their activities.

## Mission and Operations

Although it exists to enforce the drug laws of the United States, DEA operates on a worldwide basis. It presents materials to the U.S. civil and criminal justice system, or to any other competent jurisdiction, regarding those individuals and organizations involved in the cultivation, production, smuggling, distribution, or diversion of controlled substances appearing in or destined for illegal traffic in the United States.

DEA’s job is to immobilize those organizations by arresting their members, confiscating their drugs, and seizing their assets. Among its responsibilities are investigation of major narcotics violators operating at the interstate or international levels; seizure of drug-related assets; management of a national narcotics intelligence system; coordination with federal, state, and local law enforcement authorities, as well with counterpart agencies abroad; and training, scientific research, and information exchange in support of prevention and control of drug traffic.

**Liaison with other agencies and countries.** The liaison between DEA and other agencies exists at all levels, from its relationship with law-enforcement in U.S. cities, towns, and counties to its interaction with the United Nations. DEA also works with INTERPOL and other organizations on matters relating to international narcotics control. Its agents operate throughout the world, with nations who seek to reduce the flow of drugs, and against those few rogue regimes—such as the Taliban in Afghanistan prior to the U.S. victory in late 2001—who profit from the sale of illegal drugs. Exemplary of DEA’s worldwide sweep was an August 2002 *Washington Post* report that it was increasing its presence both along the Mexican border and on the other side of the planet, in Afghanistan, where it was sending 17 additional agents to help control the flow of chemicals used to process heroin.

Particularly significant is DEA’s interaction with the Federal Bureau of Investigation (FBI). As part of a federal law enforcement reorganization by the Reagan administration, the FBI in January 1982 officially joined forces with DEA so as to greatly increase federal anti-drug efforts. Up to that point, DEA had reported to the associate attorney general—who at that time happened to be future New York City Mayor Rudolph Giuliani—but thereafter it would answer to the FBI director. At the same time, FBI gained concurrent jurisdiction with DEA where drug offenses were concerned. The result was the increase of the federal anti-drug force to some 10,000 FBI and DEA agents. Two decades later, DEA, a force much smaller than the FBI, was forced to reorganize some of its efforts in light of a post-September, 2001, FBI redirection of 400 agents from drug investigations to counterterrorism.

**DEA intelligence.** From its beginning, DEA was concerned with the collection, analysis, and dissemination of drug-related intelligence through its Operations Division, which supplied federal, state, local, and foreign officials with information. Originally, the agency had just a few intelligence analysts, but as the need grew, so did the staff, such that by the end of the twentieth century, DEA intelligence personnel—both analysts and special agents—numbered nearly 700.

Along the way, demand for drug-related intelligence became so great that the DEA leadership, recognizing how overtaxed the operations division was, in August, 1992, created the Intelligence Division. The latter consists of four entities: the Office of Intelligence Liaison and Policy, the Office of Investigative Intelligence, the Office of Intelligence Research, and EPIC. The last of these, located in El Paso, Texas, served as a clearinghouse for tactical intelligence (intelligence on which immediate enforcement action can be based) related to worldwide drug movement and smuggling. Eleven federal agencies participate at EPIC in the coordination of intelligence programs related to interdiction.

**Other programs and the goals they serve.** DEA also creates, manages, and supports domestic and international enforcement programs aimed at reducing the availability and demand for controlled substances. Among its dozens of programs is Demand Reduction, operated by 22 special agents at 21 domestic field divisions to educate youth and communities as a whole, to train law-enforcement personnel, and to encourage drug-free workplaces.

Demand Reduction falls under the heading of the first of three goals DEA established late in the twentieth century, and toward which it continued to work in the early twenty-first. That first goal is to educate and enable America's youth to reject illegal drugs as well as alcohol and tobacco. Among the programs in the service of the second goal—to increase the safety of America's citizens by substantially reducing drug-related crime—are the Mobile Enforcement Teams, which work to dismantle drug organizations.

The third goal, to break foreign and domestic drug sources of supply, places DEA in collaboration with foreign governments and agencies through programs such as the Northern Border Response Force. DEA also works with other federal agencies, including the Department of Justice National Drug Intelligence Center. DEA intelligence itself serves this third goal.

#### ■ FURTHER READING:

##### BOOKS:

Levine, Michael. *Deep Cover: The Inside Story of How DEA Infighting, Incompetence, and Subterfuge Lost Us the Biggest Battle of the Drug War*. New York: Delacorte Press, 1990.

Ojeda, Auriana. *Drug Trafficking*. San Diego, CA: Greenhaven Press, 2002.

Stutman, Robert M., and Richard Esposito. *Dead on Delivery: Inside the Drug Wars, Straight from the Street*. New York: Warner Books, 1992.

##### PERIODICALS:

Lichtblau, Eric. "White House Report Stings Drug Agency on Abilities." *New York Times*. (February 5, 2003): A16.

Reddy, Anitha. "Terrorists Are Now Targets in Money-Laundering Fight." *Washington Post*. (July 25, 2002): E3.

Schmidt, Susan. "DEA to Bolster Presence along Mexican Border, in Central Asia." *Washington Post*. (August 10, 2002): A11.

##### ELECTRONIC:

Drug Enforcement Administration. <<http://www.dea.gov>> (March 13, 2003).

##### SEE ALSO

ATF (*United States Bureau of Alcohol, Tobacco, and Firearms*)

Drug Control Policy, *United States Office of National NDIC (Department of Justice National Drug Intelligence Center)*

## Dead Drop Spike

A dead drop spike is one of several types of equipment for concealing, and protecting from the elements, materials left at a dead drop. The latter term refers to the site at which an intelligence agent leaves materials—documents, film, etc.—for a handler or intelligence agent to retrieve at a later time. The handler may in turn leave money or other items for the agent to subsequently retrieve. Obviously, it is important to both parties, as well as the agency sponsoring their activity, that these materials be safe from detection, theft, or harm by the elements or animals. Hence the need for the spike and similar devices.

Used since the late 1960s, a dead drop spike typically looks like a large, fat pencil. The blunt, "eraser" end has a lid that can be unscrewed, so as to insert materials and close them up in an air- and watertight chamber. The pointed end, or spike, makes the device easy to stick into the ground—safe from detection by interlopers, but easy enough for the agent or handler to retrieve.

Another device for making a dead drop is a wallet-like waterproof pouch. Sewn into the lining are ball bearings, which ensure that the pouch will sink to the bottom of a stream or ditch rather than float away. A "clam" dead drop is a tiny metal chamber attached to a magnet, such that it can be attached to an inconspicuous place on a car or any other large object with metallic parts.

#### ■ FURTHER READING:

##### BOOKS:

Melton, H. Keith. *The Ultimate Spy Book*. New York: DK Publishing, 1996.

##### ELECTRONIC:

Dead Drop Spike. Central Intelligence Agency. <<http://www.cia.gov/cia/information/artifacts/dead.htm>> (February 1, 2003).

##### SEE ALSO

Drop

## Dead-Letter Box

A dead-letter box is a covert location where messages or other items are deposited for retrieval by other intelligence operatives. Also called a dead drop, it is most often used as a means of transferring documents and messages, but can also be used to funnel equipment and money to agents in the field.

Dead-letter boxes can be highly clandestine or in obvious places such as public trash bins, nooks in buildings, and mailboxes that can be incorporated into normal activity. The only requirements are the ability to place items into the receptacle unseen, communication between the two parties regarding drop-off and pick-up, and the ability to elude surveillance.

Although they are one of the oldest tricks in espionage, dead drops remain a useful tool. A successful dead drop requires not only the transfer of items, but also careful attention to counter-surveillance measures. A dead drop is advantageous because it is accomplished without the two parties making contact, thereby rendering surveillance of suspected persons more difficult.

In February of 2001, Robert Philip Hanssen was arrested on charges of espionage after making a dead drop of classified documents in a public park in Vienna, Virginia. Days before his arrest, Federal Bureau of Investigation agents located Russian agents placing a parcel underneath an outdoor amphitheatre in Arlington, Virginia. They retrieved and photographed the package, which contained \$50,000, the payment for the documents Hanssen was supposed to leave at the dead drop the day of his arrest. Over the course of 22 years, Hanssen, a veteran FBI counterintelligence officer, used various dead-letter boxes that he created in the New York and Washington, D.C. areas to smuggle information to Soviet (and later, Russian) agents. He was convicted of espionage and conspiracy to commit espionage and sentenced to life in prison. His final dead-letter box, code named Ellis, was underneath the supports of a park foot bridge.

#### SEE ALSO

*Tradecraft*

---

## Decontamination Methods

---

■ BRIAN HOYLE

Decontamination refers to the efforts to safeguard property and people that have been exposed to chemical, nuclear, or biological agents. The intent of decontamination is twofold. The first objective is to make the individual free from the contaminant, or, if complete removal of the agent is impossible, to reduce the concentration of the contaminant to a level that is safe for survival. The second objective is to make property safe for habitation.

Human decontamination can involve removal of a contaminant from the skin. Usually such decontamination must be done quickly, since the contaminant may be absorbed through the skin where it can cause internal

damage. In a setting such as the home, laboratory, or factory, permanent decontamination facilities can be present. For example, washrooms equipped with arm-activated water taps and antiseptic soap allow for the rapid removal of personal spills. Decontamination is also possible “in the field”, courtesy of emergency response personal decontamination kits, which can be carried with workers or soldiers.

In April, 2003, military forces of the United States, Britain, and Australia faced the prospects of chemical and biological weapons attacks by forces in Iraq, as well as decontamination resulting from the deliberate destruction of oil installations and the discovery and destruction of stored biological and/or chemical weapons. For these forces, rapid response decontamination strategies are a prudent and vital precaution during the conflict.

## Chemical Decontamination

There are a variety of decontamination methods and strategies that can be brought to bear on a chemical problem. Often, the method selected depends on the nature of the contaminant. For example, vacuuming up a spill of a powdery chemical can be a prudent step, while the same technique would be inappropriate for a liquid spill.

There are three general chemical decontamination methods. These methods involve physical, chemical, or thermal processes.

**Physical methods.** Liquid chemicals can be removed from inert surfaces or living surfaces (i.e., skin) by the use of sorbents. The sorbent can be a natural material, such as soil, diatomaceous earth, or activated charcoal, or can be synthetic (i.e., Amberlite XAD-2 and XAD-7 resins). In general, the natural materials absorb, or suck up, the liquid contaminants, while the synthetic materials adsorb contaminants. Adsorption involves the concentration of a substance from the liquid phase onto the surface of the adsorbent material due to the chemistry of the surface molecules.

The most recognizable solid absorbent is a clay material known as Fuller’s Earth. This material is commonly found in kitty litter. When solid absorbent materials like Fuller’s Earth, soil, or diatomaceous earth are used, the contaminant is usually not altered. For example, petroleum products are readily absorbed but are not changed in their character. Thus, the sorbent material becomes toxic and so must be collected and disposed of afterwards. Caution needs to be taken during the collection process, as fine dust or particles can be inhaled or stuck to exposed skin.

A different type of physical decontamination involves washing the contaminant away using another fluid like water, an alcohol, or freon. The aim here is to dilute the



A volunteer is scrubbed by hospital workers wearing biohazard suits during an Omaha, Nebraska, hospital bioterrorism decontamination drill in March 2002. AP/WIDE WORLD PHOTOS.

contaminant in the wash fluid, which should itself be collected for proper disposal. Washing is not a complete decontamination. Residual contaminant can remain behind in cracks or other hiding places. However, the use of high-pressure sprays can be an effective and rapid means of decontaminating surfaces like walls and floors.

**Chemical methods.** Chemical decontamination goes further than merely removing a contaminant from the environment. Rather, in chemical decontamination the adsorbing chemical neutralizes a contaminant. One example of chemical neutralization is the adsorption of a contaminant by material that is impregnated with an alkaline chemical. Another general example is the use of chemically reactive compounds that interact with the contaminant and change its structure into a form that is non-toxic.

A popular chemical decontamination strategy relies on the use of oxidizing agents. Bleach is a well-known example of an oxidizing agent. The use of oxidizing compounds such as calcium hypochlorite or sodium

hypochlorite inactivates a variety of chemical compounds as well as dangerous microorganisms such as bacteria and viruses.

Oxidizing agents can be wiped onto a spill and collected in an absorbent material. As well, some oxidizing agents can be incorporated into topical lotions, which are smeared onto the skin to help inactivate a chemical or biological spill.

A recent innovative example of an oxidizing agent is L-Gel. Developed at Lawrence Livermore National Laboratory, L-Gel uses potassium peroxydisulfate to deactivate a variety of biological agents, including anthrax spores and *Yersinia pestis* (the bacterium that causes plague). The thick gel is able to cling to surfaces better than water, especially to steeply sloping surfaces like walls, which keeps the decontaminant in contact with the target longer than using a straight water-based decontaminant. It is hoped that a powdered formulation of the product will soon be available for use in ventilation ducts, where clean up of chemical and biological agents is especially difficult.



During the fall of 2001, L-Gel was successfully used to decontaminate offices of Congress and at ABC News following the receipt of letters that were laced with anthrax spores.

Strong bases, such as hydroxide forms of calcium, sodium hydroxide, and potassium are other useful chemical decontaminants. These agents disrupt chemical bonds in the contaminant and so destroy the offending compounds' noxiousness.

Water is an ideal fluid for decontamination because a variety of chemically different detergents and soaps readily dissolve in water. These compounds can loosen or bind contaminants and so remove them from a surface. The friction of scrubbing also aids in decontamination of the skin during hand washing.

The different tendencies of chemicals to dissolve in water (a property known as solubility) affects the efficiency of a decontaminant. For example, a longer period of decontamination is needed when using a compound that is not readily soluble in water. This problem can be somewhat overcome by the use of microemulsions, which are essentially very small droplets of the decontaminant. The droplet coat is a material that is less water-soluble. The effect is best seen when oil is added to water. Then, a sheen of oil appears on the water, rather than a homogeneous oil-water mixture. If a contaminant is not water soluble, it will quickly partition into the hydrophobic ("water-hating") decontaminant portion of a microemulsion. This can speed up the action of a decontaminant. Microemulsions can be applied to a contaminated surface as a spray, which can be washed off later.

**Thermal methods.** Thermal decontamination is the use of heat to vaporize those chemical contaminants that will readily convert from a liquid to a gas in the presence of heat. Both water- and alcohol-based chemicals can exhibit this behavior.

Water can also be heated, even to the extent of being converted to steam. Hot water or steam treatment can be an efficient means of decontamination of greasy or oily contaminants. The use of moist heat, as in the laboratory sterilization unit called an autoclave, disrupts chemical bonds in many microorganisms, killing them. Unfortunately, certain noxious bacteria that form spores (i.e., *Bacillus anthracis*, *Clostridium* species) can, under some circumstances, survive autoclaving.

Hot air is another useful decontaminant for compounds that can be volatilized. This method is useful for situations where a spill can be isolated and treated over a longer period of time. In a battlefield situation, other more urgent methods are preferable.

## Nuclear Decontamination

Nuclear decontamination in a battlefield site, to date only applicable in the Japanese cities of Hiroshima and Nagasaki in the waning days of World War II, necessitates the

removal, burial, or storage of the contamination. However, in sites such as decommissioned nuclear power plants or weapons manufacturing facilities, the less concentrated amounts of radioisotopes that are encountered can be more systematically decontaminated.

Nuclear decontamination consists of the removal of the contaminating radioisotope. Removal can be accomplished by the use of water-soluble chemicals (i.e., alkaline permanganate, citric oxalic acid), fire-fighting foam, and even the electrochemical treatment of the contaminated surface.

## Personal Decontamination

The specter of contamination with agents, in particular biological agents, was seared into the public consciousness in the latter months of 2001. Then, U.S. citizens were subjected to terrorist attacks as letters containing *Bacillus anthracis*, the bacterium that is the cause of anthrax were mailed through the U.S. Postal Service.

The concern over the use of biological weapons has not abated since that time. Indeed, the possibility of biological attack, and so the need for rapid decontamination, was one of the paramount concerns of U.S. troops and their allies involved in the war in Iraq in the winter and spring of 2003.

Suspected exposure to an aerosol of a dangerous microorganism should be dealt with promptly. The exposed clothing should be taken off and safely contained so as not to contaminate bystanders or medical personnel. It may be necessary to destroy clothing depending on the suspected contaminant. For example, spores of the anthrax bacteria can cling to clothing and retain their potential for infection for decades. Exposed skin should be decontaminated. The best strategy is to use soap and water with diligent scrubbing for at least 30 seconds. The use of diluted household bleach is acceptable.

Decontamination in the case of biological exposure is typically done in an isolated facility, where the access of personnel is tightly controlled, and the outgoing air can be filtered to prevent the spread of the biological agent. Such facilities are even used in the battlefield setting.

In battlefield settings such as Iraq, the military can use a dried resin known as M291. This resin is a dry black carbon containing material that decontaminates by absorption and physical removal of the chemical agents from the victim. M291 resin is particularly useful for localized ("spot") decontamination of exposed skin.

**Organization of a military treatment area.** Part of military strategy in conflicts where there is a potential for the use of biological or chemical weapons, as in the Iraq conflict of 2003, is the establishment of medical treatment facilities. In the battlefield a facility is divided into two zones. One zone (the "dirty" zone) is where contaminated personnel and equipment are segregated. The other, "clean" zone is

kept free from the contaminating agents. The transition area between these zones, which is called the hotline, keeps contaminated people (including casualties) and equipment out of the clean side until decontamination is completed.

Triage, emergency treatment, and decontamination are done in the dirty zone. The emergency treatment station essentially treats patients as best as possible and stabilizes them for movement to the clean zone operation theatre, or evacuation to a hospital. Any decontamination is done in the dirty zone, with more substantive medical procedures being done in the clean zone.

## Civilian Decontamination

The National Pharmaceutical Stockpile Program in the U.S. has assembled large quantities of antibiotics, vaccines, and other medical treatment countermeasures that can be rapidly deployed. For example, in the aftermath of the anthrax attacks in the U.S. during 2001, federal and state agencies were able to quickly provide the antibiotic ciprofloxacin (Cipro) to those potentially exposed to *Bacillus anthracis*.

In the event of a large scale contamination, such as the "dusting" of anthrax spores over a metropolitan area, large numbers of casualties would likely result, as decontamination strategies for such masses of people are still in the planning stages.

## Decontamination during the Iraq War of 2003

The past deployment of chemical and biological weapons by the government of Iraq under Saddam Hussein, and the inconclusive findings of the United Nations weapons inspectors who were present in Iraq in 2002–2003, heightened concerns for the possible use of such weapons during the 2003 war between Iraq and coalition forces of the United States and the United Kingdom.

In the 1980–88 war with Iran, Iraq deployed chemical weapons that affected an estimated 100,000 Iranians, killing about 10,000 people. Even today, some 1,000 people are considered to be moderately to severely ill because of these attacks.

Another decontamination effort will be necessary to deal with the oil wells that have been set ablaze by Iraqi soldiers in the 2003 conflict. The residue given off by the blazing wells in sufficient numbers could be an environmental disaster, and is unhealthy to breathe. Unfortunately, decontamination is virtually impossible, other than to extinguish the blazes and to clean up the terrain immediately surrounding the wells once they have been extinguished.

Contamination of the drinking water supplies of southern Iraqi towns such as Safwan and Zubayr makes the

possibility of disease more immediate. Post-war decontamination efforts involved the isolation and treatment of the contaminated surface and ground waters.

### ■ FURTHER READING:

#### BOOKS:

Boss, Martha J., Dennis W. Day, and Roger F. Jones. *Biological Risk Engineering Handbook: Infection Control and Decontamination*. Boca Raton: Lewis Publishers, Inc., 2002.

Mauroni, Albert J. *America's Struggle with Chemical-Biological Warfare*. Westport, CN: Praeger Publishers, 2000.

#### ELECTRONIC:

United States Environmental Protection Agency. "Anthrax." EPAHome. January 14, 2003. <<http://www.epa.gov/epahome/hi-anthrax.htm>>(04 March 2003).

#### SEE ALSO

*Anthrax Weaponization*  
*L-Gel decontamination reagent*  
*Pathogens*

## Decryption

Decryption is simply the reverse of encryption, the process by which ordinary data, or plain text, is converted into a cipher. A cipher, often incorrectly identified as a code, is a system in which every letter of a plain text message is replaced with another letter so as to obscure its meaning. To decipher a message requires a key, an algorithm that provides the method by which the message was encrypted.

**Ciphers, algorithms, and keys.** In one of the earliest and simplest ciphers, Julius Caesar sent messages in which each letter was substituted by the letter three places after it in the alphabet. In place of *A*, then, one would use a *D*. The key for such a cipher would be simply, "Shift right by three," or something similar.

A key is an algorithm, or a method for solving a mathematical problem by using a finite number of computations, usually involving repetition of certain operations or steps. An excellent example of an algorithm is  $f(x) = y$ , a formula by which a relationship between two elements is shown on a Cartesian coordinate system. It is said that "y is a function of x," meaning that for every value of x, there is a corresponding value of y. Suppose it is established that  $2x = y$ ; then the key for the function has been established, and all possible values of x and y can be mapped.

**Brute force and weak and strong encryption.** In a simplified form, this is what occurs in decryption. The example

shown is one that could easily be solved by what are called “brute-force” means. Brute force is a method of decryption in which a cryptanalyst, lacking a key, solves a cipher by testing all possible keys. This tends to be impractical for most ciphers without the use of a computer, and for the most sophisticated modern ciphers, brute force is all but impossible.

Suppose, however, one were shown a graph with the following coordinates for  $x$  and  $y$ : 1, 2; 2, 4; 3, 6, and so on. It would be fairly easy to determine from these values, using brute force, that  $2x = y$ , even if one did not have the key. This is an example of “weak” encryption. By contrast, some of the systems in use today for encryption of bank transactions or cellular phone communications and other purposes are extremely “strong”. The ultimate example of strong encryption would be a situation in which decryption would be impossible without knowing the key.

Strong encryption is a controversial matter, due to the concerns of law-enforcement and intelligence authorities that such ciphers could be used by terrorists or other illegal groups. This has led to a move on the part of several governments, including that of the United States, to set up “key-escrow” arrangements, whereby all developers of ciphers would be required to give authorities a “back door” or key into the cipher. The government would maintain decryption keys in a secure location, and use them only when given a court order.

■ FURTHER READING:

BOOKS:

Kahn, David. *The Codebreakers: The Story of Secret Writing*. New York: Macmillan, 1967.

Kippenhahn, Rudolf. *Code Breaking: A History and Exploration*. Woodstock, NY: Overlook Press, 1999.

Levy, Steven. *Crypto: How the Code Rebels Beat the Government, Saving Privacy in the Digital Age*. New York: Viking, 2001.

Schneier, Bruce. *Secrets and Lies: Digital Security in a Networked World*. New York: John Wiley, 2000.

SEE ALSO

*Encryption of Data*  
*GSM Encryption*  
*Pretty Good Privacy (PGP)*

.....  
**Defense Information Systems  
 Agency, United States**  
 .....

The Defense Information Systems Agency (DISA) has the responsibility of planning, developing, and supporting the

C4 (command, control, communications, and computers) and information systems that serve the president of the United States and other national leaders. DISA is also responsible for Department of Defense (DOD) telecommunications and information processing facilities and systems. Included among the latter are the Global Command and Control System, or GCCS.

DISA was established in 1960 as the Defense Communications Agency. Overseen directly by the assistant secretary of defense for Command, Control, Communications (C3) and Intelligence, the agency serves the needs of the president, the vice president, the secretary of defense, the joint chiefs of staff, combatant commanders, and other DOD components under all conditions of both peace and war. As the agency responsible for maintaining defense information infrastructure, DISA ensures that this infrastructure will be interoperable with theater and tactical command and control systems, with the C4 systems of allied nations, and with any other national or international systems relevant to the DISA mission. Furthermore, DISA supports the National Communications System (NCS) in its national security emergency preparedness telecommunications functions.

Among the information and communication systems DISA manages are the Defense Message System, the Defense Information Systems Network, the Global Combat Support Systems, the Common Operating Environment, and the Global Command and Control System (GCCS). GCCS is the nation’s leading system for command and control of joint and coalition forces, and incorporates applications required by battlefield commanders to prepare and undertake military operations. Fielded at more than 625 sites globally, GCCS is networked through the highly secured private intranet of the DOD.

■ FURTHER READING:

BOOKS:

*Communications Management and Control Activity (CMCA)*. Washington, D.C.: Defense Information Systems Agency, 1995.

*The Defense Information Systems Agency (DISA): NAA, “The Three Sisters”*. Washington, D.C.: Defense Information Systems Agency, 1995.

*Operation: DISA, A Continuing Evolution*. Arlington, VA: Defense Information Systems Agency, 1996.

ELECTRONIC:

Defense Department Space Policy. Federation of American Scientists. <[http://www.fas.org/spp/military/docops/defense/d5105\\_19.htm](http://www.fas.org/spp/military/docops/defense/d5105_19.htm)> (February 22, 2003).

Defense Information Systems Agency. <<http://www.disa.mil/>> (February 22, 2003).

SEE ALSO

*Communications System, United States National DOD (United States Department of Defense)*

## Defense Nuclear Facilities Safety Board, United States

The Defense Nuclear Facilities Safety Board (DNFSB) is an independent agency of the federal government charged with overseeing the disposition of defense nuclear materials controlled by the Department of Energy (DOE). Created by Congress in 1988, DNFSB as of 2003 consisted of three members responsible for advising, and providing recommendations to, the secretary of energy.

Today there are a dozen DOE defense nuclear sites around the nation, including facilities at Oak Ridge, Tennessee, and Los Alamos, New Mexico. From the time of the development of nuclear weapons by the United States in World War II until the 1980s, the operation of these facilities had taken place without benefit of external oversight, a situation that continued even as DOE replaced the old Atomic Energy Commission in the 1970s. By the late 1980s, public health and safety concerns raised by the accumulation of hazardous materials at the increasingly aged facilities of the defense nuclear complex prompted action on the part of Congress. The latter in 1988 passed the National Defense Authorization Act, which established DNFSB.

**Activities and powers of DNFSB.** An independent agency within the executive branch of government, DNFSB provides oversight with regard to all activities within DOE's nuclear weapons complex that affect, or potentially affect, public safety. Up until the end of the cold war, the nuclear weapons complex was concerned with designing and testing weapons, and with maintaining the nation's nuclear arsenal. With the end of the cold war, and hence of the arms race it spawned, the mission of the nuclear weapons complex changed. Thenceforth, its resources were committed to cleaning up contaminated sites, dismantling nuclear weapons, storing and disposing of excess materials, and maintaining the now-reduced nuclear stockpile.

To ensure that these activities are undertaken with the strictest concern for public health and safety, DNFSB continually reviews and evaluates activities at defense nuclear facilities. The board then makes recommendations to the secretary of energy regarding specific measures it deems necessary to protect the public. DNFSB also reviews, and if necessary recommends changes to, designs for new facilities, as well as modifications to old ones. The board also has the power to undertake investigations, issue subpoenas, hold public hearings, gather data, conduct studies, and establish requirements for DOE reporting. DNFSB is in turn required to report to Congress at least once a year.

### ■ FURTHER READING:

#### BOOKS:

*Nuclear Safety: The Defense Nuclear Facilities Safety Board's First Year of Operation: Report to Congressional Requesters.* Washington, D.C.: General Accounting Office, 1991.

*Plans, Progress, and Experience to Date of the Defense Nuclear Facilities Safety Board: Hearings Before the Subcommittee on Strategic Forces and Nuclear Deterrence of the Committee on Armed Services, United States Senate, One Hundred First Congress, Second Session, March 28, 1990.* Washington, D.C.: U.S. Government Printing Office, 1990.

#### ELECTRONIC:

Defense Nuclear Facilities Safety Board. <<http://www.dnfsb.gov>> (February 22, 2003).

#### SEE ALSO

*DOE (United States Department of Energy)  
Nuclear Power Plants, Security  
Nuclear Reactors  
Nuclear Regulatory Commission (NRC), United States*

## Defense Security Service, United States

The Defense Security Service (DSS) serves the Department of Defense (DOD) in a number of capacities, conducting personnel security investigations, providing industrial security products and services, and offering security training to DOD personnel, contractors, and employees of other government agencies. Its most significant undertakings are the Personnel Security Investigations (PSI) Program; the Industrial Security Program (ISP); and the Security Education, Training, and Awareness Program.

Established as the Defense Investigative Service on January 1, 1972, the service changed to its present name in November 1997 in order to more accurately reflect the breadth of its mission. Oversight comes from the assistant secretary of Defense for Command, Control, Communications, and Intelligence. As of 2003, DSS employed some 2,600 persons throughout the United States, with a much smaller contingent in Europe. About half of its personnel roster was comprised of special agents responsible for undertaking approximately half a million PSIs per year. Another 230 employees were involved in the ISP program, working with more than 11,000 contractors involved in research, development, and other classified projects outsourced to specially screened entities in the private sector.

**Background investigations.** The PSI program of the DSS oversees background investigations on military, civilian, and contractor personnel affiliated with DOD. PSIs are used to determine the suitability of an individual for entrance into the armed services, for access to classified information, and for appointment to sensitive positions within DOD. PSIs conducted by DSS special agents are submitted to the agency's Personnel Investigations Center at Fort Meade, Maryland, where they are processed. When completed, PSIs are sent to the appropriate DOD adjudicative facility, which makes the determination as to the individual's suitability. DSS is thus purely a reporting and screening agency, and has no power to choose or reject individuals for positions within DOD.

The work of processing security clearances, the most prominent service of DSS, has also provided the occasion for a number of frustrations. In July 2000, the agency experienced the breakdown of a \$100 million computer system, thus temporarily bringing to a halt its background checks. Also in that month, a review panel that included representatives of DSS came under fire for approving an award to Loral Space & Communications Corporation "for outstanding security performance and practices." In 1996, Loral had forwarded a report on a Chinese rocket to the Chinese government without first obtaining State Department clearance, a situation that had led to a grand jury investigation. The backlog of security clearance investigations forced DSS to turn to civilian contractors for help. In June 2002, DOD investigators learned that one of the firms DSS had used, Government Business Services Group, may have submitted false reports to DSS and claimed to have completed work it had not done. As of fiscal year 2004, DOD had transferred responsibility for conducting most background checks from DSS to the Office of Personnel Management (OPM).

**Other DSS programs.** Under the ISP heading in DSS are three industrial security programs, the largest of which is the National Industrial Security Program, or NISP. DSS representatives working in the NISP oversee security at cleared contractor facilities, and assist the contractor's staff in formulating and maintaining security programs. The other two ISP sections are the Arms, Ammunition, and Explosives (AA&E) Program, which provides protection for munitions, and the Critical Infrastructure Program (CIP), which oversees systems vital to the operation of DOD. Additionally, the Defense Industrial Security Clearance Office (DISCO) in Columbus, Ohio, processes, issues, and maintains ISP facility and personnel clearances.

The Security, Education, Training, and Awareness Program includes instruction in counterintelligence and other areas. Training takes place at the DSS Academy, or DSSA, in Linthicum, Maryland, where some 10,000 students from DOD and the defense industry learn core security disciplines that integrate training in CI and information systems. Education is provided through combinations of formal classroom teaching, computer-based learning, and correspondence, distance, or tele-training.

In the realm of counterintelligence, the DSS Counterintelligence Office, established in May 1993, seeks to integrate an awareness of counterintelligence with DSS core mission areas. Its aims are to infuse the defense workforce with counterintelligence knowledge, to increase awareness of counterintelligence throughout DOD and the contractor base, and to assist those it trains in recognizing and reporting intelligence collection activities conducted by foreign powers or groups.

#### ■ FURTHER READING:

##### PERIODICALS:

- Barr, Stephen. "Defense Department Agrees to Have OPM Take Over Background Checks." *Washington Post*. (February 5, 2003): B2.
- Pincus, Walter. "Computer Shutdown Hits Defense Security Service; Backlog of Background Checks Grows." *Washington Post*. (July 8, 2000): A10.
- . "A Pentagon 'Embarrassment': Loral Wins, Is Stripped of Award for Security Practices." *Washington Post*. (July 19, 2000): A21.
- Pound, Edward T. "Keeping Secrets Secret." *U.S. News & World Report*. (June 3, 2002): 22.

##### ELECTRONIC:

- Defense Security Service. <<http://www.dss.mil/>> (February 22, 2003).

##### SEE ALSO

*Classified Information*  
*Counter-Intelligence*  
*DOD (United States Department of Defense)*  
*Security Clearance Investigations*

---

## Delta Force

---

Delta Force is one of the two principal United States counter-terrorism units, the other being the Naval Special Warfare Development Group, formerly known as Seal Team Six. Created in 1977 by Colonel Charles "Charlie" Beckwith, Delta Force is headquartered at Fort Bragg, North Carolina. Little is known about the elite unit, which is highly trained and well equipped with state-of-the-art weaponry, airborne insertion equipment, and other forms of technology. Delta Force has participated in a multitude of counter-terrorist actions from 1979 onward.

**Formation.** In forming Delta Force, which was activated in November 1977, Beckwith drew on his experience with the British 22nd Regiment Special Air Service (SAS), with which he worked in an exchange program in 1962 and 1963. Despite the heavy influence of SAS, with which it

often trains—along with France’s GIGN, Germany’s GSG-9, Israel’s Sayeret Matkal/Unit 269, and Australia’s Special Air Service Regiment—Delta Force has its own, very distinct and unique, character.

The official name of Delta Force is 1st Special Forces Operational Detachment-Delta, meaning that it is organizationally part of the Special Forces, themselves an elite fighting unit under U.S. Special Operations Command. Yet, Delta Force is housed apart from the Special Forces at Bragg, and in appearance they are unlike any regular army in the world. Many wear their hair well beyond regulation length, and they often work in civilian clothes. Unlike Special Forces or the Rangers, from which many of their personnel are drawn, Delta Force has no distinct outward uniform or insignia.

In addition to special-warfare units, Delta Force members may come from other parts of the army or even other branches of the military. The group conducts limited recruiting, and undertakes specialized efforts to acquire personnel possessing unique and valuable skills. A soldier who speaks an obscure language, or who possesses special technical abilities may be approached and directly recruited by a representative from Delta Force.

**Facilities and equipment.** Little is known about the inside of the Delta Force compound, though it reportedly has extensive training facilities that include numerous shooting areas (both for battle at close proximity, and for sniping at longer range), an Olympic-sized swimming pool, a dive tank, and a three-story wall for climbing. The compound also reportedly includes a facility for hostage-rescue training, known as the “House of Horror” and modelled on the “Killing House” of SAS.

Delta Force uses an array of equipment, some of it specialized for the group’s unique mission. For example, personnel conduct extensive airborne training, including specialized HAHO (high altitude-high opening) and HALO (high altitude-low opening) jumps. HALO work requires a soldier to fall through the air a considerable distance without the opened chute to break his fall, and thus he must keep his hands above his head. However, this can cause much of the blood to flow out of the arms, leaving the soldier to operate at less than full capacity during the first few minutes after he touches ground. To solve this problem, Delta Force arranged to have specially built parachute rigs that allow them to keep their hands at their sides during descent.

**Delta Force operations.** Delta Force works closely with other services and federal agencies, particularly the Central Intelligence Agency. Its first deployment was an inauspicious one, the attempted rescue of hostages held in the U.S. embassy in Teheran on April 25, 1980. In any case, the failure of this mission, which ended with a fatal helicopter crash before the special unit (composed of elite fighters from several military services) even reached Teheran, had little to do with Delta Force.

Delta Force also participated in the U.S. invasion of Grenada in 1983, and in 1984 and 1985 conducted assaults on jetliners hijacked by terrorists in the Middle East. During the opening moments of Operation Just Cause in Panama in 1989, it rescued Kurt Muse, an American citizen held in a Panamanian prison. In the Persian Gulf War, Delta Force served initially as bodyguards for top U.S. officers, and later as part of an effort to locate and destroy mobile SCUD missile launchers in the Iraqi desert. Delta Force also served in Task Force Ranger in Somalia (1993); a variety of operations associated with the Balkan wars of 1992–2000; Operation Enduring Freedom in Afghanistan in 2001–2002; and Operation Iraqi Freedom in 2003.

#### ■ FURTHER READING:

##### BOOKS:

- Beckwith, Charlie A., and Donald Knox. *Delta Force*. San Diego: Harcourt Brace Jovanovich, 1983.
- Bennett, Richard M. *Espionage: An Encyclopedia of Spies and Secrets*. London: Virgin Books, 2002.
- Griswold, Terry, and D. M. Giangreco. *Delta, America’s Elite Counterterrorist Force*. Osceola, WI: Motorbooks International, 1992.
- Haney, Eric L. *Inside Delta Force: The Story of America’s Elite Counterterrorist Unit*. New York: Delacorte Press, 2002.
- Landau, Alan M., et. al. *U.S. Special Forces: Airborne Rangers, Delta, and U.S. Navy SEALs*. Osceola, WI: MBI, 1999.

##### SEE ALSO

- ADFGX Cipher*  
*Asymmetric Warfare*  
*Australia, Intelligence and Security*  
*Carter Administration (1977–1981), United States National Security Policy*  
*DOD (United States Department of Defense)*  
*France, Counter-Terrorism Policy*  
*Germany, Counter-Terrorism Policy*  
*Guerilla Warfare*  
*Israel, Counter-terrorism Policy*  
*SEAL Teams*  
*Special Operations Command, United States*  
*United States, Counter-Terrorism Policy*

---

## Department of State Bureau of Intelligence and Research, United States

---

#### ■ CARYN E. NEUMANN

The Bureau of Intelligence and Research (INR) draws on intelligence from a range of sources to provide continuous independent analysis of global events to the secretary of

state and other diplomatic policymakers. Established in 1946 to aid United States foreign policy and national security goals, the bureau's location within the Department of State means that it has more knowledge of policy ingredients in a given estimative question than the analysts at the Central Intelligence Agency (CIA) or the various military intelligence agencies. Accordingly, INR is a member of the National Counterintelligence Policy Board (NCPB), provides briefings to the entire intelligence community, and helps oversee all U.S. government activities overseas.

The primary objective of INR is to serve the Department of State by ensuring that intelligence activities support foreign policy plans. It acts as the focal point in the department for ensuring policy review of sensitive counterintelligence and law enforcement activities, while also analyzing geographical and international boundary issues. In support of the State Department's responsibility for the oversight of all U.S. government activities overseas, INR coordinates the agency's activities relating to intelligence, security, counterintelligence, investigative, and special operations. It sits on the NCPB and participates in national security community decision-making on visa denial, intelligence sharing, as well as the requirements and evaluation for data collection in all intelligence disciplines.

INR staff draws on all-source intelligence, diplomatic reporting, its own public opinion polling, and interaction with U.S. and foreign scholars to provide early warning and in-depth analysis of events and trends. On an annual basis, INR analysts examine about two million reports to produce more than 6500 written assessments that are read by officials within the State Department, embassy personnel, the White House, the National Security Council, the Department of Defense, Congress, and the intelligence community.

The officers and analysts of INR draw upon a vast amount of knowledge. The bureau consists of about 300 employees who are organized into 19 offices that mirror the other divisions of the State Department. The employees, three-fourths of whom are Civil Service and one-fourth of whom come from the Foreign Service, blend both continuity and country-specific knowledge. They utilize thirty-six different languages to integrate new data and insights into their reports. Seventy-one percent of INR officials hold advanced degrees, with over a quarter possessing doctorates. On average, INR analysts and officers have spent six years within the bureau and 13 years studying the country or issue for which they are responsible.

Perhaps the most significant contribution that INR makes to national security comes through its estimative intelligence. The estimative views of INR help compose the National Intelligence Estimates (NIEs) produced by the National Intelligence Council (NIC). While most NIC officers come from the CIA, INR officials are part of the quarter of NIC analysts that are drawn from other parts of the government. When few facts are available, INR analysts help fill in the picture to predict what might be or might happen.

The major security lapses of the recent past such as the failure to predict the true strength of Soviet military defenses and the surprise testing by India of a nuclear bomb have led to calls to improve U.S. intelligence capabilities. Reinvigorating the diminished place of the State Department, particularly INR, in collecting and evaluating intelligence has been proposed as one means of bettering national security. Policymakers need estimative intelligence to help them understand the more diffuse and ambiguous threats and opportunities of the post-Cold War world and the specific knowledge offered by INR has historically served as a valuable national security component. Accurate and timely intelligence is the critical first line of defense against danger and INR provides exactly this material.

#### ■ FURTHER READING:

##### BOOKS:

Ford, Harold P. *Estimative Intelligence: The Purposes and Problems of National Intelligence Estimating*. Lanham, MD: University Press of America, 1993.

##### ELECTRONIC:

United States Intelligence Community. "Department of State: Bureau of Intelligence and Research." <[http://www.intelligence.gov/1-members\\_state.shtml](http://www.intelligence.gov/1-members_state.shtml)> (March 23, 2002).

##### SEE ALSO

*CIA (United States Central Intelligence Agency)*  
*Department of State, United States*  
*Intelligence Community*  
*National Intelligence Estimate*  
*NIC (National Intelligence Council)*  
*Terrorist Organization List, United States*

---

## Department of State, United States

---

#### ■ JUDSON KNIGHT

The Department of State is a cabinet-level division of the United States government concerned with the planning, conduct, and management of U.S. foreign policy and foreign relations. The secretary of state is the highest-ranking member of the cabinet, and traditionally, secretaries of state have been among the most powerful members of the government. The State Department includes six major sections, each headed by an under secretary of state, concerned with Political Affairs; Economic, Business, and Agricultural Affairs; Arms Control and International Security; Global Affairs; Management; and Public

Diplomacy and Public Affairs. The department manages some 250 diplomatic posts worldwide, along with a number of special offices, bureaus, and agencies tasked to address issues such as counterterrorism, arms control and proliferation, organized crime, and narcotics trafficking. Also notable is the U.S. Agency for International Development (USAID), through which the United States extends assistance to nations recovering from disasters or trying to improve their political and/or economic conditions.

## History

Oldest executive department of the federal government, the State Department grew out of the Committee of Secret Correspondence, established by the Continental Congress in 1775. Its first chairman was Benjamin Franklin. Over the next 14 years, the office went through a number of name changes until, on September 15, 1789, Congress designated it the Department of State.

Initially, the department had a range of domestic responsibilities, such as operation of the mint, issuing of patents, and regulation of immigration, that have long since passed on to other departments and bureaus. John Jay, who had served as secretary for foreign affairs (as the title of the chief American diplomat was called between 1781 and 1789) served as acting secretary until President George Washington's appointee, Thomas Jefferson, took office as secretary of state in 1790.

For the next 80 years, appointment as secretary of state tended to be set aside for persons distinguished in politics or government, but not necessarily diplomacy. These included future presidents Jefferson, James Madison, James Monroe, John Quincy Adams, Martin Van Buren, and James Buchanan, as well as other notable leaders, mostly from Congress, including Henry Clay, Daniel Webster, John C. Calhoun, and William H. Seward.

In those early years, America remained largely isolated from the rest of the world, and the State Department saw little activity except in times of war, or when the federal government sought to acquire lands. In the years leading up to the Civil War, Washington sought to ensure European support for the union, a critical matter since Great Britain and France depended to a large degree on cotton from the South.

The State Department only emerged as a vital component of U.S. policy after the Spanish-American War of 1898, as the United States acquired territories overseas and became increasingly involved in foreign affairs. The first modern secretary of state was John Hay, who, during his tenure (1898–1905), negotiated several treaties toward the building of the Panama Canal, and promoted open access to trade in China.

The fact that President Woodrow Wilson went personally to Paris to serve as U.S. negotiator at the post-World War I peace conference shows that even in 1919, the State Department had yet to acquire its present significance. Only in the wake of World War II did the United

States, having fully left isolationism behind, begin to place a heavy emphasis on its State Department.

In the early years of the Cold War, three strong secretaries of state—George C. Marshall (1947–49), Dean Acheson (1949–53), and John Foster Dulles (1953–59)—helped forge the framework of U.S. policy. Among the components of that policy were containment of Communism, support for liberal democracies in Europe, and promotion of U.S. interests in the third world. The latter strategy involved not only alliances with pro-American movements, but also assistance. In service of this aim, President John F. Kennedy and Secretary of State Dean Rusk (1961–69) in 1961 created USAID and the Peace Corps. (The latter became an independent agency in 1981.)

Since the Kennedy era, the importance of the secretary of state has risen or fallen depending on the administration. The power of Henry Kissinger's (1973–77) influence was substantial, and was derived from his position as national security advisor, an office he held concurrent with his appointment at state for some time. Among the more active secretaries of State are two from the turn of the twentieth century: Madeleine Albright (1997–2001) and Colin Powell (2001—), who were also the first female and African American, respectively, to hold the position.

## Duties and Structure

The State Department has its headquarters in a marshy area, nicknamed Foggy Bottom, near the Potomac River in Washington, D.C. Hence the name "Foggy Bottom" is sometimes used as a metonym for the department itself. The Department's entire foreign affairs budget—including U.S. representation overseas, foreign assistance programs, foreign military training, and efforts against international crime—comprised just one percent of the federal budget, and cost each American citizen about twelve cents a day.

To promote and protect U.S. interests abroad, the State Department works to assure peace and stability in regions of vital interest; to create jobs at home by opening markets overseas; to help developing nations establish stable economies that encourage growth and opportunities; and to bring nations together in order to address global issues such as disease, terrorism, humanitarian crises, environmental threats, weapons proliferation, and nuclear smuggling.

As the lead U.S. foreign affairs agency, the State Department has the primary role in leading interagency coordination in developing and implementing foreign policy; managing the U.S. foreign affairs budget and other foreign affairs resources; leading and coordinating U.S. representation abroad; conducting negotiations and concluding agreements; and coordinating and supporting the international activities of U.S. agencies and officials.

The department maintains embassies in about 180 nations, or all but about a dozen countries (among which are states such as Cuba, Iran, and North Korea), and also has representation with non-governmental organizations



such as the United Nations (UN) or NATO (North Atlantic Treaty Organization). Among the services provided by the department, both as a whole and through its various embassies, are protection and assistance for U.S. citizens living or traveling overseas; assistance for U.S. businesses in the international marketplace; coordination and support for international activities of other U.S. agencies, as well as other diplomatic efforts, including official visits overseas and at home; and keeping the public informed regarding U.S. foreign policy and international relations.

**State Department leadership.** The significance of the secretary of state, from an official standpoint, is indicated by the fact that he or she is fourth in the line of succession for the presidency, after the Speaker of the House, vice president and president *pro tempore* of the Senate. As chief diplomat, the secretary of State is the president's principal advisor on foreign affairs, and sits on the National Security Council (NSC) and other important committees. In practice, the importance of the secretary's position depends on the significance accorded to the office, or its holder, by the President. The secretary's relationship with Congress is also important to his or her success, because all authorization of funding for foreign policy initiatives comes from Capitol Hill. Additionally, the Senate must approve all treaties and ambassadorial appointments.

The Office of the Secretary of State includes a number of key positions and personnel, among them the Deputy Secretary and Executive Secretariat. The latter is responsible for inter- and intradepartmental coordination on foreign policy initiatives. Additionally, attached to the Secretary's office are a number of important bureaus, including the Policy Planning Staff, which provides the Secretary with independent policy planning and analysis; the Office of Protocol, whose duties include planning and hosting diplomatic events; the Office of the Coordinator for Counterterrorism, which works to improve coordination of U.S. counterterrorism efforts with those other governments; and a variety of other offices.

There are other bureaus that, while not attached to the Office of the Secretary, report directly to the Secretary. These include the Office of the Permanent Representative to the United Nations; the Bureau of Legislative Affairs; the Bureau of Intelligence and Research, part of the State Department's participation in the U.S. Intelligence Community; the Office of Inspector General, which independently audits Department activities; the Office of the Legal Adviser; and the Counselor of the Department, who advises the secretary on major foreign policy problems.

**Under secretaries and their responsibilities.** There are six under secretaries in the State Department. The under secretary of political affairs manages international crises, and is responsible for looking after U.S. political, economic, and security interests in the nation's bilateral relations. The section has six geographic bureaus—for African, East Asian and Pacific, European and Eurasian, Near

Eastern, South Asian, and Western Hemisphere affairs—headed by assistant secretaries. Also within Political Affairs is the Bureau of International Organization Affairs, which coordinates U.S. policy within organizations such as the UN and NATO.

The under secretary for Economic, Business, and Agricultural Affairs is the senior economic official at the State Department, and addresses issues involving economics and trade. Duties include coordination of State Department efforts on behalf of U.S. businesses, as well as working with the Commerce Department to promote American economic interests abroad.

Within the purview of the under secretary for Arms Control and International Security are the Bureau of Arms Control, the Bureau of Political-Military Affairs, the Nonproliferation Bureau, and the Bureau for Verification and Compliance. As a whole, this section of the State Department is concerned with global U.S. security policy, primarily in the areas of nonproliferation, arms control, regional security and defense relations, arms transfers, and security assistance.

The under secretary for Management oversees a number of offices responsible for management improvement, security, information technology, support services, consular affairs, training, and other personnel matters. Among its sections is the Bureau of Diplomatic Security, which manages the Counterterrorism Rewards Program and the Overseas Security Advisory Council.

Included under the heading of the Global Affairs Group, headed by another under secretary, are offices that address a variety of global issues. Among these are the Bureau of Democracy, Human Rights, and Labor; the Bureau of International Narcotics and Law Enforcement Affairs; the Bureau of Oceans and International Environmental and Scientific Affairs; and the Bureau of Population, Refugees, and Migration.

Finally, the under secretary for Public Democracy and Public Affairs is concerned with cultural and educational exchanges, as well as international information programs. Its Bureau of Public Affairs helps Americans understand U.S. foreign policy, while the Bureau of Economic and Cultural Affairs attempts to foster mutual understanding between the United States and other nations. The Office of International Information Programs sponsors a variety of information and strategic communication initiatives involving print, electronic media, and the Internet.

## ■ FURTHER READING:

### BOOKS:

- Craig, Gordon Alexander, and Francis J. Lowenheim. *The Diplomats, 1939–1979*. Princeton, NJ: Princeton University Press, 1994.
- Gore, Albert. *Department of State and U.S. Information Agency: Accompanying Report of the National Performance Review*. Washington, D.C.: U.S. Government Printing Office, 1993.

Plischke, Elmer. *U.S. Department of State: A Reference History*. Westport, CT: Greenwood Press, 1999.

*Principal Officers of the Department of State and United States Chiefs of Mission, 1778–1990*. Washington, D.C.: U.S. Department of State, 1991.

*“Reinventing Government”: Change at State*. Washington, D.C.: U.S. Department of State, Bureau of Management, 1993.

*State 2000: A New Model for Managing Foreign Affairs: Report of the U.S. Department of State Management Task Force*. Washington, D.C.: U.S. Government Printing Office, 1993.

#### ELECTRONIC:

U.S. Agency for International Development. <<http://www.usaid.gov/>> (April 25, 2003).

U.S. Department of State. <<http://www.state.gov/>> (April 25, 2003).

#### SEE ALSO

*Coordinator for Counterterrorism, United States Office Department of State Bureau of Intelligence and Research, United States*

*Diplomatic Security (DS), United States Bureau FEST (United States Foreign Emergency Support Team) International Narcotics and Law Enforcement Affairs (INL), United States Bureau*

*Terrorist Organization List, United States*

---

## DIA (Defense Intelligence Agency)

---

■ JUDSON KNIGHT

The Defense Intelligence Agency (DIA) coordinates intelligence activities within the U.S. Department of Defense (DOD). Established in 1961, DIA has faced a number of territorial challenges both from the intelligence components of the three major armed services, as well as from other intelligence agencies. DIA, which has some 7,000 civilian and military employees worldwide, is headquartered at the Pentagon in Washington, D.C. Its director is a three-star military officer who serves as principal military intelligence advisor to the secretary of defense and the chairman of the Joint Chiefs of Staff (JCS).

### Background

Despite the congressional passage of the 1958 Defense Reorganization Act, which created unified military commands, the U.S. Army, Navy, and Air Force each guarded their intelligence organizations. As a result, DOD leadership did not receive consistent, reliable intelligence, a shortcoming that contributed to the failed April 1961 invasion of Cuba. Even before that, President John F. Kennedy complained in his 1961 State of the Union speech about “a

growing gap between decision and execution, between planning and reality.” In February, 1961, Defense Secretary Robert S. McNamara informed JCS of his decision to create a Defense Intelligence Agency, and instructed the Joint Chiefs to develop a plan for the new organization, which began operation on October 1, 1961.

The intention behind DIA was that it should serve as a tight union, rather than a loose confederation, of defense intelligence and counterintelligence activities, so as not to increase the bureaucratic layering within an already thickly populated defense intelligence community. Its director would report to the secretary of defense through JCS. Upon establishment of DIA, the services transferred various intelligence functions to it gradually, so as to maintain the pace of ongoing activities. The job of DIA would be to collect, process, evaluate, analyze, integrate, produce, and disseminate military intelligence for DOD.

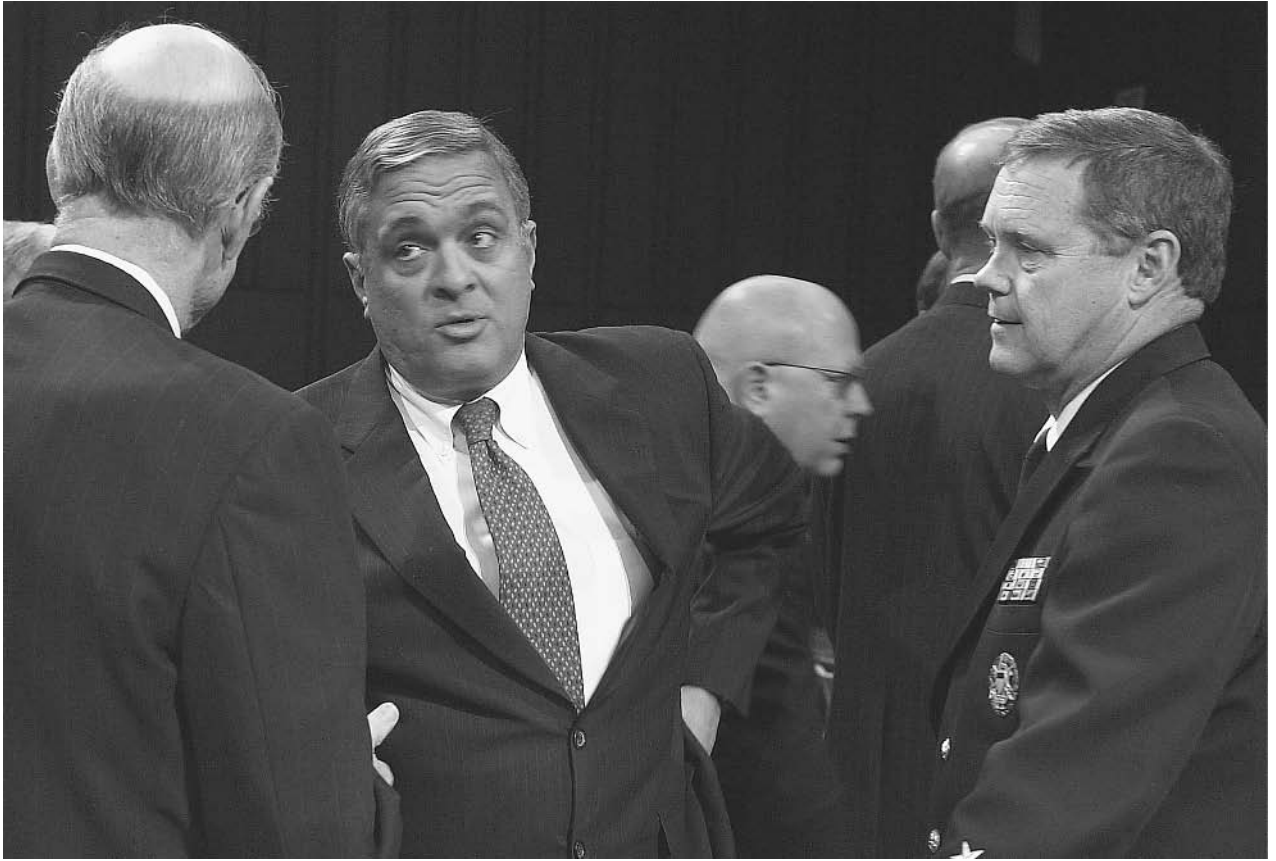
As DIA has admitted in its own official history, its attempts to establish itself as the central military intelligence organization within DOD met with continuing resistance from the military services during the 1960s. First, the services retained their own military intelligence organizations, and their leadership was often wary of sharing intelligence with a relative newcomer. The Vietnam War, in which DIA was tasked with helping to account for missing or captured military personnel, particularly tested the abilities of the fledgling agency.

By the mid-1970s, DIA had gained considerable funding, but its budget of more than \$200 million annually made it a target for congressional inquiries, particularly by the Pike Committee, the House equivalent of the more well-known Church Committee in the Senate. Within the Intelligence Community, Admiral Stansfield Turner, director of the Central Intelligence Agency (CIA) criticized DIA’s inability to effectively coordinate military intelligence activities on the part of the various services.

Executive Order 12036, signed by President James E. Carter on January 24, 1978, restructured the Intelligence Community and brought DIA’s responsibilities into focus. The agency was subsequently reorganized into five directorates, concerned with production, operations, resources, external affairs, and J-2 (joint intelligence) support. During the 1980s, a DIA white paper series on Soviet military capabilities gained wide respect in the intelligence community.

Soon after the Iraqi invasion of Kuwait in August, 1990, DIA established a 24-hour intelligence management center focusing on intelligence relating to the crisis. Some 2,000 DIA personnel participated in Operation Desert Storm, primarily through the National Military Joint Intelligence Center (NMJIC), which DIA established at the Pentagon to integrate intelligence from the war front. On the ground in Kuwait and Iraq, DIA personnel worked closely with military combat units.

In 1992, the Armed Forces Medical Intelligence Center and the Missile and Space Intelligence Center, both controlled by the Army for decades, became part of DIA. The



Vice Admiral Thomas Wilson, right, confers with CIA Director George Tenet, center, after Tenet's testimony before the Senate Armed Services Committee in March 2002, to discuss the threat to U.S. interests around the world by al Qaeda. AP/WIDE WORLD PHOTOS.

following year saw a thoroughgoing reorganization of DIA as part of the general military downsizing that followed the end of the Cold War. In October 1995, DIA established the Defense HUMINT [Human Intelligence] Service, or DHS.

## Structure of DIA

Though DIA was conceived as a military organization, the majority of its personnel today are civilians. The director, however, is always a three-star officer—a lieutenant general or vice admiral. (The only exceptions were General Donald V. Bennett, director from 1969 to 1972, a four-star general, and Dennis M. Nagy, a civilian who served as acting director during the fall of 1991.) In addition to the Command Element, which includes leadership and support staff, DIA consists of three major sections: Analysis, Intelligence Operations, and Support Services.

Within the Analysis section are the directorates for Analysis and Production; Intelligence, Joint Staff (J2); and Policy Support. Analysis and Production manages key components of the intelligence cycle for DOD, its leadership, and its services. The directorate for Intelligence, Joint Staff (J2) supports the chairman of JCS and other uniformed leaders by providing a national-level focal point for crisis intelligence support. Within it is the Defense

Intelligence Network, which operates a closed circuit DOD news network modeled on commercial news networks such as CNN, as well as INTELINK, a classified Internet. Policy Support works with the Office of the Secretary of the Defense, as well as the National Security Council and State Department.

Intelligence Operations includes the directorate for Intelligence Operations and the Central MASINT Organization. These are concerned, respectively, with human intelligence and measurement and signatures intelligence. Within the directorate for Intelligence Operations is DHS, the Defense HUMINT Service.

Under Support Services are the directorates for Administration and Information Systems and Services. Among the administration sections is the Counterintelligence and Security Activity, which works to counter foreign intelligence threats, conducts security and suitability interviews, and assists the Federal Bureau of Investigation and military investigative organizations in criminal and counterintelligence investigations. Information Systems and Services supports a number of activities, including the operation of the Joint Worldwide Intelligence Communications System, a high-bandwidth system that makes possible full-motion video teleconferencing and data exchange among major intelligence nodes.

In addition to these main sections, DIA also includes the Program Management directorate, under which is the Military Intelligence Board, the DIA director's advisory committee. Also outside the main sections of DIA is the Joint Military Intelligence College, which is accredited to award bachelor's and master's degrees in intelligence and strategic intelligence.

#### ■ FURTHER READING:

##### BOOKS:

*Disposition of Production Records of the Defense Intelligence Agency: A NARA Evaluation.* Washington, D.C.: National Archives and Records Administration, 1996.

*Intelligence Agencies: Personnel Practices at CIA, NSA, and DIA Compared with Those of Other Agencies.* Washington, D.C.: General Accounting Office, 1996.

Richelson, Jeffrey T. *The U.S. Intelligence Community*, fourth edition. Boulder, CO: Westview Press, 1999.

Scanlon, Charles Francis. *In Defense of the Nation, DIA at Forty Years.* Washington, D.C.: Defense Intelligence Agency, 2002.

##### ELECTRONIC:

Defense Intelligence Agency. <<http://www.dia.mil/>> (April 14, 2003).

Defense Intelligence Agency. Federation of American Scientists. <<http://www.fas.org/irp/dia/>> (April 14, 2003).

##### SEE ALSO

*Air Force Intelligence, United States*

*Bay of Pigs*

*DOD (United States Department of Defense)*

*HUMINT (Human Intelligence)*

*INSCOM (United States Army Intelligence and Security Command)*

*Intelligence*

*Intelligence Community*

*Intelligence, United States Congressional Oversight*

*Internet*

*Kennedy Administration (1961–1963), United States National Security Policy*

*Measurement and Signatures Intelligence (MASINT)*

*National Military Joint Intelligence Center*

*NMIC (National Maritime Intelligence Center)*

*NRO (National Reconnaissance Office)*

*NSA (United States National Security Agency)*

*Persian Gulf War*

essential, the contact telephone number can be obtained with a device called a dial tone recorder.

In a touch-tone telephone, each digit from 0 through 9 produces two tones when the particular key is pressed. Each tone has a particular wavelength (i.e., height of the peak and trough of the wave) and a frequency (i.e., the number of waves and troughs per unit area). One of the tones is from a low group, which represents the rows on the telephone keypad. The other tone is from a high group, which represents the columns on the keypad. The function of the dial tone decoder is to decipher the tone pairs and match up the combination with the row and column location on the telephone keypad. In an operating phone, this information is passed to a switch, which routes the signal to the phone line, allowing the call to proceed.

A dial tone decoder is also a standard feature of touch tone telephones, and makes the phone capable of converting the numerical and symbolic information that is entered using the phone's keypad into a signal that can complete the transmission.

A decoder can also detect a busy signal. In espionage, this allows the eavesdropper to find out whether the telephone being monitored is in use. Dial tone decoders can also route the dial tones to a personal computer equipped with an infrared port, as the electrical impulses of the tones can be converted to infrared radiation. Thus, a computer can be used to record the activity of a telephone over time, including the numbers dialed during that period.

Instances of assassination via cellular telephones equipped with a decoder and an explosive device have occurred in contested areas of the Middle East in the late 1990s. When the subject answered the telephone, a code was entered that triggered a blast. Detection of the code by the dial tone decoder triggers the explosive device. In this way, attacks were carried out from remote locations. In an Islamist militant group Hamas attack in July 2002, five Americans and four Israelis were killed at the Hebrew University in Israel after a bomb placed in a backpack in the university cafeteria was remotely detonated by cell phone.

In police investigations, dial tone decoders are routinely used for intelligence gathering, and are also used by telephone repair crews to verify phone numbers.

#### ■ FURTHER READING:

##### BOOKS:

Goleniewski, Lillian. *Telecommunication Essentials.* Boston: Addison Wesley Professional, 2001.

Ledwidge, Michael S. *Bas Connection.* New York: Simon & Schuster, 2001.

Proakis, John G. *Digital Communications.* New York: McGraw-Hill, 2001.

##### SEE ALSO

*Microphones*

## Dial Tone Decoder

Telephone conversations are sometimes surreptitiously taped using microphones or other bugging devices. These devices run the risk of being detected. In some intelligence-gathering tapings, however, the contact telephone number may yield information that is as valuable as the actual conversation. If the content of a conversation is not

*Telephone Recording Laws*  
*Telephone Scrambler*

## Digital Watermarking.

SEE *Steganography*.

## Diplomatic Security (DS), United States Bureau

■ CARYN E. NEUMANN

The Bureau of Diplomatic Security (DS) is the law enforcement and security arm of the United States Department of State. Created on November 4, 1985, it bears responsibility for ensuring the safety of Americans who are serving their government in embassies and consulates overseas as well as protecting foreign dignitaries who visit the United States. It also investigates crimes involving passport and visa fraud.

Diplomats traditionally have given little concern to security. Aware of this shortcoming and the increasing risks of terrorism, the secretary of state convened an Advisory Panel on Overseas Security under the chairmanship of retired Admiral Bobby R. Inman. The 1985 Inman Report warned that growing security demands at home and abroad required the Department of State to establish a professional law enforcement service with its own structure for personnel recruitment, advancement, and assignment. In light of the danger of mob attacks and terrorist sabotage upon U.S. embassies, the panel also recommended that more physically secure sites and buildings replace a large number of diplomatic facilities around the world. The new service would initiate and direct this relocation and building program.

Upon its creation, DS began providing protective details based on the level of threat to selected foreign officials within the U.S. as well as to American ambassadors and other officials overseas. It does not protect visiting heads of state but, in response to specific threats made against them, will guard foreign missions in the U.S. through agreements with state and local law enforcement authorities. On the average, DS participates in more than 150 foreign and domestic dignitary details each year. By the mid-1990s, DS personnel had thwarted twenty-two assassinations in progress, eighteen of them overseas. The service also evacuated embassies in nations on the verge of collapse.

To monitor and analyze all international and domestic terrorism matters, DS relies upon Intelligence and Threat Analysis (ITA) to link with the U.S. intelligence community. Besides issuing a classified Daily Security

Brief to senior DS and State Department officers, ITA produces two annual publications. *Significant Incidents of Political Violence against Americans* is a narrative and statistical compendium of all acts of terrorism and political violence against U.S. interests in a given year. *Terrorist Tactics and Security Procedures* offers case studies of specific terrorist attacks or security developments that affect the safety of Americans abroad. ITA also distributes the semiannual Security Environment Threat List (SETL), which helps DS prioritize resource allocation by categorizing political risks and crime at all U.S. missions overseas.

DS also attempts to deter the efforts of foreign intelligence agencies to compromise U.S. employees. It investigates crimes involving passport and visa fraud while examining the backgrounds of employees, applicants, contractors, and others who seek access to Department of State information or facilities. Additionally, the service investigates personnel security matters with counterintelligence ramifications in conjunction with the National Counterintelligence Center.

DS generally receives little notice and is probably best known for its regular bulletins of security suggestions for U.S. business representatives overseas. By working with the Department of State's Overseas Security Advisory Council as well as American embassies and consulates, it provides current information about precautions that can provide some degree of protection by serving as psychological and practical deterrents to would-be terrorists. This information includes warnings about new crime strategies, such as kidnappers who first appear as vendors operating carts across from the homes of Americans, as well as time-honored advice like recommendations to vary daily travel routes.

The volume of DS investigations has steadily increased each year. In light of the current high risk of terrorist activity, the demand for DS service will likely continue to grow.

### ■ FURTHER READING:

#### BOOKS:

- Katz, Samuel M. *Relentless Pursuit: The DSS and the Manhunt for the al-Qaeda Terrorists*. New York: Tom Doherty Associates, 2002.
- Smith, G. Davidson. *Combating Terrorism*. New York: Routledge, 1990.
- United States Department of State, Bureau of Diplomatic Security. *Countering Terrorism: Security Suggestion for U.S. Business Representatives Abroad*. Washington, D.C.: Department of State, 1999.

#### ELECTRONIC:

- United States Department of State. "Bureau of Diplomatic Security." March 29, 2003 <<http://www.ds.state.gov>> (March 29, 2003).

#### SEE ALSO

*Architecture and Structural Security*

*Assassination*  
*Department of State, United States*  
*Security Clearance Investigations*  
*Terrorism, Intelligence Based Threat and Risk Assessments*  
*Terrorist Organization List, United States*

## Directed Energy Weapons.

SEE *Defense Initiative and National Missile Defense.*

## Dirty Bombs.

SEE *Russian Nuclear Materials, Security Issues.*

---

## Dirty Tricks

---

Dirty tricks are clandestine activities carried out by a covert-action group to discredit, destabilize, or eliminate an opposing regime, one of its agencies or departments, or an individual. A type of covert operation, dirty tricks include everything from the spreading of false rumors to sabotage, overthrow, and assassination.

**American dirty tricks.** The history of dirty tricks practiced by the United States Central Intelligence Agency (CIA) is a long one. Among the most significant examples in this extensive catalogue are the many attempts to undermine or neutralize Cuban dictator Fidel Castro. These ranged from large-scale conspiracies such as assassination plans and the Bay of Pigs invasion to bizarre brainstorming at the fringes of practicability. An example of the latter was a plot to introduce a substance that would cause Castro's famous beard to fall off, thus presumably eliminating his machismo and thus his credibility with the Cuban people.

Castro was far from the only foreign leader targeted by CIA dirty tricks. Another example was Chilean president Salvador Allende, who steered his nation toward Marxism in the early 1970s. The CIA bribed members of the Chilean Congress, and employed a number of means to foment unrest in Chile. Evidence gathered by the Church Committee of the U.S. Senate indicates that the CIA may have been behind the truckers' strike of 1972–73 that helped spawn the coup in which Allende lost his life and General Augusto Pinochet took power.

**Soviet dirty tricks.** Though CIA dirty tricks, such as those that were revealed in the course of the Iran-Contra hearings in the late 1980s, are legendary for their cunning, the

United States is hardly the only nation that has employed dirty tricks in its covert operations. Another example is the Soviet Union, whose KGB operatives were past masters at such tactics ranging from disinformation to assassination. The Soviets, of course, had the advantage—at least, in countries where their system gained control—of being able to suppress all undesirable information. Yet, even before the fall of the Soviet empire, extensive information on Soviet activities was available.

To cite one example among many of those noted by British journalist Chapman Pincher in *The Secret Offensive* (1985) the Soviets sought to strike back at Egyptian president Anwar Sadat for his increasingly pro-American acts by printing leaflets attacking him as a U.S. puppet. These tracts, which the CIA traced to the Soviets, but which were purportedly issued by Muslim fundamentalists, helped fan the flames of the Muslim Brotherhood, which had Sadat assassinated in 1981. The KGB also provided the Weathermen, a U.S. radical group in the 1960s, with money and other forms of assistance through Cuban intermediaries, and Soviet support for terrorist groups attempting to destabilize western Europe during the 1970s and 1980s is well-documented.

### ■ FURTHER READING:

#### BOOKS:

- Bennett, Richard M. *Espionage: An Encyclopedia of Spies and Secrets.* London: Virgin Books, 2002.
- Carney, John T., and Benjamin F. Schemmer. *No Room for Error: The Covert Operations of America's Special Tactics Units from Iran to Afghanistan.* New York: Ballantine, 2002.
- Pincher, Chapman. *The Secret Offensive.* New York: St. Martin's, 1985.
- Richelson, Jeffrey T. *The U.S. Intelligence Community,* third edition. Boulder, CO: Westview Press, 1995.

#### SEE ALSO

- Black Ops*  
*Church Committee*  
*CIA (United States Central Intelligence Agency)*  
*Iran-Contra Affair*  
*KGB (Komitet Gosudarstvennoi Bezopasnosti, USSR Committee of State Security)*

---

## Disinformation

---

### ■ MARTIN J. MANNING

Disinformation is mostly commonly described as false information created by governments in wartime for military purposes and by totalitarian governments for political



University students protest against possible fraud in the 2000 elections in Peru. The word "SIN" refers to Peru's national intelligence agency, which allegedly used dirty tricks and intimidation to give the incumbent President Alberto Fujimori an unfair advantage over his opponent, Alejandro Toledo. Fujimori later resigned and Toledo gained the presidency. AP/WIDE WORLD PHOTOS.

purposes in peacetime. Rumors, lies, and other forms of disinformation were made public by the Soviet Union to discredit the United States, the latter being the context in which the word is generally applied. The KGB coined the Russian word *dezinformatsiya*; it came into the English language as disinformation. The technique of disinformation goes back at least to 1918 with the end of World War I. Disinformation as a KGB weapon began in 1923 when I. S. Inshlikht, deputy chairman of the GPU, then the name of the KGB, proposed the establishment of a special disinformation office to conduct active intelligence operations.

**Soviet active measures.** Soviet active measures refer to the influence operations organized by the Soviet government. These include white, gray, and black propaganda, as well as disinformation. White propaganda was created by the Information Department of the Communist Party and included those publicly identified Soviet channels as Radio Moscow, *Novosti*, and pamphlets and magazines as well as official Soviet government statements. Gray propaganda was organized by the International Department of the Communist Party and used such channels as the

foreign Communist Parties and the network of international Soviet fronts. Black propaganda was prepared by the KGB and included agents of influence, covert media placements, and until 1959, assassinations. Forgeries and disinformation were used by the Soviets in all modes. The first effective disinformation campaign was during the Korean Conflict. This was a major Soviet disinformation campaign that generated media attention. The Americans were accused of going into Korean villages during the Korean conflict (1950–1953) and shooting villagers, or killing them with biological weapons and chemical warfare. In fact, the Soviets used anthrax in Korea to kill men, women, and children, and then blamed it on the Americans.

An attempt is now underway with the Cold War History Project at the Woodrow Wilson International Center for Scholars, Smithsonian Institution, in Washington, DC, to counter this account, especially through the work of Katherine Weathersby who discovered that Soviet documents obtained through a Japanese researcher belied these rumors and accusations. The issue re-surfaced in the book *United States and Biological Weapons: Secrets of the Early Cold War and Korea* (Indiana University Press,

1999) by Stephen Endicott and Edward Hagerman. Endicott was the son of one of the men who helped to disseminate the disinformation campaign, James Endicott.

On September 9, 1982, President Ronald Reagan designated the United States Information Agency to lead an inter-departmental effort to counter Soviet propaganda and disinformation. For an advisory body, the administration created the Active Measures Working Group in 1981 to bring together the information the various agencies held to counter Soviet disinformation and forgery. It served as a clearinghouse to expose such information and it had permission to use classified documents and any other resources that were required to meet this goal. The Working Group was chaired by the State Department with representatives from State, Central Intelligence Agency, Defense Intelligence Agency, Arms Control and Disarmament Agency, United States Information Agency, and the Defense and Justice Departments. The Working Group ended in 1991, two years after the collapse of the Soviet Union.

**AIDS disinformation campaign.** A major effort for the Working Group was the AIDS disinformation campaign, a controversial topic that had basis as a Soviet disinformation campaign. A sensational disinformation story appeared with allegations that the United States deliberately created AIDS in the laboratory to use it as a weapon. The KGB started the story in 1985 with placements in both Soviet and foreign newspapers; by September, 1986, it became a major campaign when an English language paper that actually originated in East Berlin carried the story. "AIDS: Its Nature and Origin," was distributed at the Non-Aligned Movement Summit in Harare, where it contained pseudo scientific verbiage, but the only evidence linking the origin of AIDS to U.S. military laboratories was the following unfounded statement: "The first appearance of AIDS exactly coincides with the opening of a P-4 laboratory at Fort Detrick [Maryland]—taking into account the incubation period. This is also indicated by the fact that the spreading of AIDS to the world emanated from New York, a city in the neighbourhood of Fort Detrick. The assumption that AIDS is a product of the preparation of biological warfare can therefore quite plainly be expressed."

The Soviet disinformation campaign accused the U.S. government of creating the AIDS virus as a weapon against black people and the story quickly appeared worldwide, despite U.S. protests that Fort Detrick, in Maryland, was hundreds of miles from New York. In April 1987, U.S. Surgeon General C. Everett Koop advised the Soviets that if this campaign continued, "direct U.S.-Soviet collaboration on AIDS research would be impossible." The KGB then began winding down the worldwide campaign, but other countries continued to endorse the disinformation. In Africa, stories circulated for years that the United States created the AIDS virus. The U.S. Information Service (USIS, USIA overseas) staff responded with accurate information that countered these charges and defused the situation. In

Pretoria, South Africa, and in Lilongwe, Malawi, USIS information was able to refocus the media on AIDS prevention rather than on false blame.

**World Trade Center attacks.** After the terrorist attacks of September 11, 2001, a disinformation campaign originated that 4000 Jewish persons did not show up for work at the World Trade Center on that day. Authorities have not determined the origin of the disinformation, but have concluded that its source was probably from an Arabic region, as the circulated disinformation did not mention the fact that the hijackers were Arabic. This was the first recorded account of an urban legend that has swept the Arab world, and no facts in it have ever been substantiated. The disinformation appears to be based on concern expressed by the Israeli government for the fate of 4,000 Israeli residents in New York, a small number of whom worked at the World Trade Center. Within a matter of days it was no longer 4,000 Israelis who were supposed not to have turned up to work, but 4,000 Jewish persons; then reports appeared that no Jewish persons died on September 11. In fact, many Jewish Americans died in the attack, as well as four Israeli citizens—two in the World Trade Center and two on hijacked planes, according to the Israeli Foreign Ministry.

In August, 2002, the U.S. Government countered allegations that Abdul Salem Zayef, the former ambassador to Pakistan, had been tortured and killed in captivity at the United States' Guantanamo detention center in Cuba. After the U.S. Embassy in Islamabad alerted the Department of State that the story was appearing in the Urdu press and that allegations were being broadcast as fact on state-controlled media, the State Department worked with elements in the Department of Defense to track how the disinformation was being disseminated, and to prepare guidance. In April, 2003, the Embassy in Islamabad also countered allegations about damage to the Adhamiya Mosque in Baghdad, which houses the Imam Abu Hanifa, with relevant CENTCOM news releases and information given for a story in the *New York Times*. Additionally, in April 2003, the U.S. Embassy in Beirut, Lebanon, responded to allegations about "tranquilizer chemical weapons" with the Department of Defense's statement that "Incapacitating agents are agents that put people to sleep by slowing the nervous system considerably. The Department of Defense does not possess any incapacitating agents and has no plans to conduct research in this area."

**Depleted uranium.** A Gulf War disinformation campaign that began when a South African minister spoke to the media about the supposed genocide caused by the use of uranium depletion weapons in the 1991 Persian Gulf War. This disinformation was started by Minister Doug Rokke in a presentation to members of the South African Parliament on January 31, 2001, when he made a number of



assertions about depleted uranium. Media reports quoted him saying that he knew only one person from his team who was not sick from depleted uranium exposure, and represented that tests revealed 5,000 times the permissible level of uranium in his body. Rokke was presented as the Department of Defense's (DOD) expert on depleted uranium and the director of the Pentagon's depleted uranium project. His comments resulted in a renewed fear about the effects of spent uranium depletion weapons.

In order to correct the record, the Defense Department revealed Rokke as a private citizen not affiliated with the U.S. Department of Defense. Following the war, Rokke was attached for duty to assist technical experts in the recovery and decontamination of radioactive material and equipment. The team of approximately 10 people was led, not by Rokke, but by a civilian from the Army Munitions and Chemical Command (AMCCOM). Rokke's primary role was to facilitate the recovery operations by ensuring the team had the proper support. In the following years, Rokke reported varying numbers of ill or dead co-workers. DOD staff compiled a list of 29 names of people Rokke reported to be on "his team." Staff members were able to interview 22 of them. Approximately 15 of the 29 people Doug Rokke had identified actually worked on depleted-uranium contaminated vehicles. Two of the 29 had died, however, neither of these two veterans was named as having worked with depleted uranium.

**Iraqi propaganda.** Early in 2003, the White House issued "Apparatus of Lies: Saddam's Disinformation and Propaganda, 1990–2003" (Washington, D.C.: U.S. Department of State, 2003) compiled by State and Defense Department disinformation specialist Todd Leventhal. This report highlighted the apparatus used by Saddam Hussein and his cadres to deceive the Iraqi people and the international community. The oppressive and totalitarian nature of Saddam Hussein's regime enabled this deception. This regime, which became expert at obfuscation during the 1991 Persian Gulf War, had more than a decade to perfect these practices before it was finally toppled by the allied forces in March and April, 2003.

In December, 1998, when United Nations weapons inspector Richard Spertzel became exasperated by Iraqi evasions and misrepresentations, he confronted Rihab Taha, the woman the Iraqis identified as the head of their biological weapons program and asked her directly, "You know that we know you are lying. So why do you do it?" She replied: "Dr. Spertzel, it's not a lie when you are ordered to lie." In January, 2003, Taha refused to be interviewed by U.N. weapons inspectors, but after Operation Iraqi Freedom, Taha surrendered to U.S. authorities on May 12, 2003.

In their disinformation and propaganda campaigns, the Iraqis used elaborate ruses and obvious falsehoods, covert actions and false on-the-record statements, and sophisticated preparation and spontaneous exploitation

of opportunities. Iraq has used four types of campaigns to promote its propaganda and disinformation:

- **Crafting tragedy:** To craft tragedy, the regime places civilians close to military equipment, facilities, and troops, which are legitimate targets in an armed conflict. The Iraqi regime openly used both Iraqis and foreigners as human shields during the Gulf War, eventually bowing to international pressure and releasing many of them. Iraq also placed military equipment next to or inside mosques and ancient cultural treasures. Finally, it has deliberately damaged facilities and attributed the damage to coalition bombing, and has attempted to pass off damage from natural catastrophes, such as earthquakes, as the result of bombing.
- **Exploiting suffering:** To exploit suffering, Saddam Hussein blamed starvation and medical crises—often of his own making—on the United Nations or the United States and its allies. The Iraqi regime caused or actively ignored hardship and then aggressively exploited the Iraqi people's suffering. During the last decade, the Iraqis have aggressively promoted the false notion that depleted uranium—a substance that is relatively harmless and was used for armor-piercing munitions during the Gulf War—has caused cancers and birth defects among Iraqis. Scientific evidence indicates that any elevated rates of cancer and birth defects are most likely due to Iraqi use and testing of chemical weapons.
- **Exploiting religion:** Experts know that Saddam Hussein was a non-religious man from a secular—even atheistic—party. In order to exploit religious sentiments, he adopted expressions of faith in his public pronouncements, and the Iraqi propaganda apparatus erected billboards and distributed images showing him in other acts of piety—all while his regime prevented citizens from engaging in religious pilgrimages. Inflammatory disinformation designed to incite Muslims against its adversaries has also been used.
- **Corrupting public records:** To corrupt the public record, the Iraqi regime used a combination of on-the-record lies, covert placements of false news accounts, self-inflicted damage, forgeries, and fake interviews.

Other main tools of Iraqi disinformation included restricting journalists' movements; false claims or disclosures; false man-in-the-street interviews; self-inflicted damage; on-the-record lies; covert dissemination of false stories; censorship; edited or old television footage and images; and fabricated documents. Recent U.S. government reports, including "A Decade of Defiance and Deception," documented these deceptions regarding UN resolutions and weapons inspections. In order to raise awareness of the many other Iraqi forms of deception, particularly those likely to be repeated, "Apparatus of Lies" examined the facts behind Iraqi disinformation and propaganda since 1990. The U.S. Defense Department countered these disinformation tactics by embedding over 300 world journalists with United States Marines during Operation Iraqi Freedom in March-April, 2003.

The author wishes to acknowledge Herb Romerstein for his contributions to this article.

*Iraqi Freedom, Operation (2003 War against Iraq)  
Persian Gulf War  
Propaganda, Uses and Psychology*

## ■ FURTHER READING:

### BOOKS:

Bittmann, Ladislav. *The KGB and Soviet Disinformation*. Washington: Pergamon-Brassey's International Defense Publishers, 1985.

Romerstein, Herbert. *Soviet Active Measures and Propaganda: "New Thinking" and Influence Activities in the Gorbachev Era*. Toronto, Canada: Mackenzie Institute for the Study of Terrorism, Revolution, and Propaganda; Washington, D.C.: National Intelligence Book Center, 1989.

Shultz, Richard H., and Roy Godson, *Dezinformatsia*. Washington: Pergamon-Brassey's International Defense Publishers, 1984.

U.S. Congress. House. Permanent Select Committee on Intelligence. *Soviet Active Measures: Hearings*. 97th Congress, 2d Session. Washington, D.C.: GPO, 1982.

U.S. Congress. Senate. Committee on Foreign Relations. Subcommittee on European Affairs. *Soviet Active Measures: Hearings*. 99th Congress, 1st Session. Washington, D.C.: GPO, 1985.

U.S. Department of State. *Active Measures: A Report on the Substance and Process of Anti-U.S. Disinformation and Propaganda Campaigns*. Washington, D.C.: The Department, 1986.

———. *A Report on Active Measures and Propaganda, 1986–87*. Washington, D.C.: The Department, 1987.

———. *A Report on Active Measures and Propaganda, 1987–1988*. Washington, D.C.: Department, 1989.

### PERIODICALS:

Douglass, Joseph D. "The Growing Disinformation Problem," *International Security Review* 4 (1981): 333–353.

Kux, Dennis. "Soviet Active Measures and Disinformation: Overview and Assessment," *Parameters, Journal of the U.S. Army War College* 15, no. 4: 19–28.

McDonnell, Sharon. "In From the Cold," *American Journalism Review* (June 1995): 16–17.

### OTHER:

Romerstein, Herbert. "Disinformation as a KGB Weapon in the Cold War." Prepared for a Conference on Germany and Intelligence Organizations: The Last Fifty Years in Review, sponsored by Akademie fur Politische Bildung Tutzing, June 18–20, 1999.

U.S. Information Agency. *Soviet Active Measures in the Era of Glasnost*. Prepared at the request of the U.S. House of Representatives, Committee on Appropriation, for presentation at a hearing on March 8, 1988, by Charles Z. Wick, Director, United States Information Agency. (Washington, 1988).

### SEE ALSO

*Iraq War: Prelude to War (The International Debate over the Use and Effectiveness of Weapons Inspections.)*

## DNA

### ■ JULI BERWALD

Because of the uniqueness of every human's DNA and the ubiquity of DNA in cells, this genetic molecule has become an important tool for the identification of individuals, both in forensics and security applications. Deoxyribonucleic acid (DNA) consists of two twisted strands of polymers, made up of mononucleotide units. Each nucleotide is composed of three separate parts: a 2-deoxyribose sugar ("2-deoxy-" because the hydroxyl or -OH group of the ribose sugar is missing from the second carbon position on the sugar ring), a phosphate, and one of the four bases: adenine (A), guanine (G), cytosine (C), thymine (T). The deoxyribose sugar and phosphate are linked by phosphodiester bridges in such a way as to form an unbranched polynucleotide chain. According to the Watson-Crick model, which was published in 1953, the DNA molecule consists of two such polynucleotide chains which are complementary but not identical and which spiral around an imaginary common axis. The two strands are antiparallel, meaning that the phosphodiester links between the deoxyribose units read in opposite directions designated 5' to 3' on one chain and 3' to 5' on the other. The bases, which are perpendicular to the helix axis, protrude at regular intervals from the two spiral sugar phosphate strands, and reach into the interior of the helix. The strands are annealed together by hydrogen bonds between the bases of opposite strands and for correct annealing to occur a purine (adenine or guanine) on one strand must pair with a pyrimidine (thymine or cytosine) on the other. Within the constraints of the double helix, hydrogen bonds can only form between adenine and thymine (A:T) and between guanine and cytosine (G:C). Through this pairing, the arrangement of bases along one strand determines that of the other and the genetic information is thus coded in these base sequences.

The most commonly described DNA structure is that of the right-handed Watson-Crick double helix, also known as B-DNA, which has a diameter of 20Å. The double helix is not symmetrical and has a broad groove and a narrow groove between the chains, known respectively as the major and minor grooves. Adjacent bases are separated by 3.4Å along the helix axis and related by a rotation of 36° which causes the helix structure to repeat after 10 residues on each chain, that is at intervals of 34Å. DNA is, however, a dynamic molecule whose structure can vary and there are two other commonly found DNA conformations, each with slightly different dimensions.



An FBI official holds a chart of the Combined DNA Index System (CODIS), a computerized database that allows law enforcement officers from around the country to compare DNA genetic evidence taken from convicted felons and gathered in unsolved cases. AP/WIDE WORLD PHOTOS.

The DNA molecule contains all of the genetic information for every organism. Within a cell, DNA is organized into long strands called chromosomes. Every chromosome contains many thousands of different genes. A gene is a functional segment of DNA that codes for a specific protein. During protein synthesis, a portion of DNA is translated into a complementary strand of ribonucleic acid (RNA), which is further transcribed into a sequence of amino acids. A sequence of three nucleotides is required to code for one amino acid and chains of amino acids are further modified outside the nucleus of the cell into the proteins. There are approximately 50,000 different types of proteins in the human body and they either perform tasks or synthesize molecules required for the biological activity that sustains life. The DNA in every individual, therefore, is the source of information that directs all of the biological functions in the body.

The DNA molecule is inherited by every cell and every individual. In asexual reproduction, the DNA in chromosomes is unwound and duplicated before the cell divides. Both daughter cells receive exact copies of the parent cell's DNA. In sexual reproduction, a portion of the DNA is inherited from both the female and the male parent. In

humans, there are 23 pairs of chromosomes in the genome. During meiosis, which forms the sex cells or gametes (the egg in females and the sperm in males), the chromosomal pairs separate and each gamete receives 23 unpaired chromosomes. When a sperm fertilizes an egg, its 23 unpaired chromosomes are paired with the 23 unpaired chromosomes in the egg and the resulting zygote contains a unique set of paired chromosomes.

#### SEE ALSO

*DNA Fingerprinting*  
*DNA Recognition Instruments*  
*DNA Sequences, Unique*

## DNA Fingerprinting

DNA fingerprinting is the term applied to a range of techniques that are used to show similarities and dissimilarities between the DNA present in different individuals.

DNA fingerprinting is an important tool in the arsenal of forensic investigators and intelligence officers. In an era when plastic surgery can be used to alter a terrorist's appearance, DNA fingerprinting allows for positive identification not only of body remains, but also of suspects in custody. DNA fingerprinting can also link physical evidence from incidents that occur in different parts of the world.

Sir Alec Jeffreys at the University of Leicester developed DNA fingerprinting in the mid 1980s. The sequence of nucleotides in DNA is similar to a fingerprint, in that it is unique to each person. DNA fingerprinting is used for identifying people, studying populations, and forensic investigations.

## Historical Uses of DNA Fingerprinting

Jeffreys was first given the opportunity to demonstrate the power of DNA fingerprinting in March of 1985 when he proved a boy was the son of a British citizen and should be allowed to enter the country. In 1986, DNA was first used in forensics. In a village near Jeffreys' home, a teenage girl was assaulted and strangled. No suspect was found, although body fluids were recovered at the crime scene. When another girl was strangled in the same way, a 19-year-old caterer confessed to one murder but not the other. DNA analysis showed that the same person committed both murders, and the caterer had falsely confessed. Blood samples of 4582 village men were taken, and eventually the killer was revealed when he attempted to bribe someone to take the test for him.

The first case to be tried in the United States using DNA fingerprinting evidence was of African-American Tommie Lee Edwards. In November 1987, a judge did not permit population genetics statistics that compared Edwards to a representative population. The judge feared the jury would be overwhelmed by the technical information. The trial ended in a mistrial. Three months later, Andrews was on trial for the assault of another woman. This time the judge did permit the evidence of population genetics statistics. The prosecutor showed that the probability that Edwards' DNA would not match the crime evidence was one in ten billion. Edwards was convicted.

DNA fingerprinting has been used repeatedly to identify human remains. In Cardiff, Wales, skeletal remains of a young woman were found, and a medical artist was able to make a model of the girl's face. She was recognized by a social worker as a local run-away. Comparing the DNA of the femur of the girl with samples from the presumptive parents, Jeffreys declared a match between the identified girl and her parents. In Brazil, Wolfgang Gerhard, who had drowned in a boating accident, was accused of being the notorious Nazi of Auschwitz, Josef Mengele. Disinterring the bones, Jeffreys and his team used DNA fingerprinting to conclude that the man actually was the missing Mengele.

In addition to forensics, DNA has been used to unite families. In 1976, a military junta in a South American country killed over 9000 people, and the orphaned children were given to military couples. After the regime was overthrown in 1983, Las Abuelas (The Grandmothers) determined to bring these children to their biological families. Using DNA fingerprinting, they found the families of over 200 children.

DNA has been used to solve several historical mysteries. On July 16, 1918, the czar of Russia and his family were shot, doused with sulfuric acid, and buried in a mass grave. In 1989, the site of burial was uncovered, and bone fragments of nine skeletons were assembled. DNA fingerprinting experts from all over the world pieced together the puzzle that ended in a proper burial to the Romanov royal family in Saint Petersburg in 1998.

## The Mechanics of DNA Fingerprinting

The nucleus of every cell in the human body contains deoxyribonucleic acid or DNA, a biochemical molecule that is made up of nearly three-billion nucleotides. DNA consists of four different nucleotides, adenine (A), thymine (T), guanine (G), and cytosine (C), which are strung together in a sequence that is unique to every individual. The sequence of A, T, G, and C in human DNA can be found in more combinations or variations than there are humans. The technology of DNA fingerprinting is based on the assumption that no two people have the same DNA sequence.

The DNA from a small sample of human tissue can be extracted using biochemical techniques. Then the DNA can be digested using a series of enzymes known as restriction enzymes, or restriction endonucleases. These molecules can be thought of as chemical scissors, which cut the DNA into pieces. Different endonucleases cut DNA at different parts of the nucleotide sequence. For example, the endonuclease called *Sma*I cuts the sequence of nucleotides CCCGGG between the third cytosine (C) and the first guanine (G).

After being exposed to a group of different restriction enzymes, the digested DNA undergoes gel electrophoresis. In this biochemical analysis technique, test samples of digested DNA are placed in individual lanes on a sheet of an agarose gel that is made from seaweed. A separate lane contains control samples of DNA of known lengths. The loaded gel is then placed in a liquid bath and an electric current is passed through the system. The various fragments of DNA are of different sizes and different electrical charges. The pieces move according to their size and charge with the smaller and more polar ones traveling faster. As a result, the fragments migrate down the gel at different rates.

After a given amount of time, the electrical current in the gel electrophoresis instrumentation is shut off. The gel is removed from the bath and the DNA is blotted onto a

piece of nitrocellulose paper. The DNA is then visualized by the application of radioactive probe that can be picked up on a piece of x-ray film. The result is a film that contains a series of lines showing where the fragments of DNA have migrated. Fragments of the same size in different lanes indicate the DNA has been broken into segments of the same size. This demonstrates a similarity between the sequences under test.

Different enzymes produce different banding patterns and normally several different endonucleases are used in conjunction to produce a high definition banding pattern on the gel. The greater the number of enzymes used in the digestion, the finer the resultant resolution.

In DNA fingerprinting, scientists focus on segments of DNA in which nucleotide sequences vary a great deal from one individual to another. For example, five to ten percent of the DNA molecule contains regions that repeat the same nucleotide sequence many times, although the number of repeats varies from person to person. Jeffreys targeted these long repeats called variable number of tandem repeats (VNTRs) when he first developed DNA fingerprinting. The DNA of each person also has different restriction fragment sizes, called restriction fragment length polymorphisms (RFLPs), which can be used as markers of differences in DNA sequences between people. Today, technicians also use short tandem repeats (STRs) for DNA fingerprinting. STRs are analyzed using polymerase chain reaction or PCR, a technique for mass-producing sequences of DNA. PCR allows scientists to work with degraded DNA.

**Use as a forensic tool.** DNA fingerprinting is now an important tool in the arsenal of forensic chemists. It is used in forensics to examine DNA samples taken from a crime scene and compare them to those of a suspect. Criminals almost always leave evidence of their identity that contains DNA at the crime scene—hair, blood, semen, or saliva. These materials can be carefully collected from the crime scene and fingerprinted

Although DNA fingerprinting is scientifically sound, the use of DNA fingerprinting in courtrooms remains controversial. There are several objections to its use. Lawyers who misrepresent the results of DNA fingerprints may confuse jurors. DNA fingerprinting relies on the probability that individuals will not produce the same banding pattern on a gel after their DNA has been fingerprinted. Establishing this probability relies on population statistics. Each digested fragment of DNA is given a probability value. The value is determined by a formula relating the combination of sequences occurring in the population. There is concern that not enough is known about the distribution of banding patterns of DNA in the population to express this formula correctly. Concerns also exist regarding the data collection and laboratory procedure associated with DNA fingerprinting procedures. For example, it is possible that cells from a laboratory technician could be inadvertently amplified and run on the gel. However, because each person has a unique DNA sequence

and this sequence cannot be altered by surgery or physical manipulation, DNA fingerprinting is an important tool for solving criminal cases.

## ■ FURTHER READING :

### BOOKS:

- Griffiths, A., et al. *Introduction to Genetic Analysis*, 7th ed. New York: W.H. Freeman and Co., 2000.
- Jorde, L. B., J. C. Carey, M. J. Bamshad, and R. L. White. *Medical Genetics*, 2nd ed. Mosby-Year Book, Inc., 2000.
- Klug, W., and M. Cummings. *Concepts of Genetics*, 6th ed. Upper Saddle River: Prentice Hall, 2000.
- Watson, J. D., et al. *Molecular Biology of the Gene*, 4th ed. Menlo Park, CA: The Benjamin/Cummings Publishing Company, Inc., 1987.

### ELECTRONIC:

- The University of Washington. "Basics of DNA fingerprinting." <<http://www.biology.washington.edu/fingerprint/dnaintro.html>>(March 4, 2003).

### SEE ALSO

- DNA Recognition Instruments*  
*DNA Sequences, Unique*  
*Fingerprint Analysis*  
*Genomics*  
*Retina and Iris Scans*

## DNA Recognition Instruments

■ AGNIESZKA LICHANSKA

DNA recognition instruments allow rapid identification of the origin of DNA in an environmental or medical sample. Recognition of the source of DNA is important in pathogen (disease-causing agent) identification in public health surveillance, and diagnostic and military applications.

DNA recognition instruments utilize two main methods for DNA detection and identification, nucleic acid hybridization and polymerase chain reaction (PCR). Hybridization of nucleic acids allows differentiation of sequences that differ by as little as one base pair by using high temperature washes that remove partially matched DNA strands. Hybridization relies on the fact that single stranded DNA reforms a double stranded helix with a complementary strand. The method requires a single stranded target (unlabeled) and probe (labeled with a radioactive or fluorescent tag to detect signal). PCR-based detection in modern instruments is based on specificity provided by primers required for DNA amplification and fluorescent probes to detect the product in real time.



A technician places a gene chip into one of the photo lithography machines shown at a production facility in California. Gene chips are dime-sized pieces of glass infused with DNA fragments that allow researchers to study how and why genes react to various stimuli. AP/WIDE WORLD PHOTOS.

**New technologies for DNA recognition.** The standard methods used in diagnostics are not rapid enough for the immediate identification of pathogens in a case of a biological attack either on military personnel or civilians. Engineers and biologists, therefore, are designing new technologies to make DNA recognition rapid, robust, with increased sensitivity of the assays and improved identification of positive samples. Optical identification methods are primarily used in PCR-based instruments; however, new magnetic and electrochemical methods were developed for hybridization-based assays.

**Hybridization-based technologies.** Chip-based hybridization assays, where the target DNA is spotted onto a glass or plastic slide and a single stranded DNA probe is used to detect it, were developed recently by a number of companies. Technology allows placement of thousands of DNA molecules on the slide, but detection of the specific reaction is often lacking sensitivity. As a result, a number of research teams and commercial companies are researching better ways to identify a positive signal.

One breakthrough came with the implementation of electrical conductivity as a detection method. This method relies on the use of electrodes with gaps of 30–50nm

in size, containing single stranded DNA molecules (oligonucleotides) immobilized on their surface (capture probes) and gold oligonucleotide nanoparticles allowing detection of electrical currents resulting from hybridization. Both oligonucleotides bind to the target sequence when the electrode is immersed in a solution containing target molecules. A modification of this method is the use of signal amplification by using a photographic solution as developed by a Northwestern University team. A salt wash before the addition of photographic developer removes mismatches and the silver coated gold particles can be easily visualized. The chip is then scanned using a flatbed scanner, removing the need for expensive equipment. This method is highly sensitive and very fast. It is able to detect concentrations of DNA (100 times more sensitive than conventional detection methods), in one to three minutes.

A modification of this method was developed in 2002 and incorporates nanoparticle probes that in addition to gold particles, have Raman dye-label (for example Cy3, Cy5, or Texas Red). Detection of these probes can be either by Raman spectroscopy or by using a flatbed scanner to detect silver enhancement. By using multiple labels one is able to design chips detecting multiple target sequences (multiple pathogens).

**Hybridization-based instruments.** The great advantage of hybridization-based instruments is the fact that they do not require any DNA amplification, are highly sensitive and give rapid results.

Scientists in industry are currently producing instruments that are based on measuring electrical conductivity. One is known as the eSensor. The system consists of bioelectronic chips, reader, and special software. The chips contain capture probes and signaling probes. After an interaction with a target sequence, signaling probes induce electric current, which is detected and interpreted by the sensor's software. This instrument can perform a number of assays simultaneously. A second instrument is directly based on the technology from the Northwestern University group, using a method of conductivity detection that was modified to amplify the signal from gold particles by using a photographic developer solution to coat the gold particles. Although this instrument currently requires a large space, work is underway to design a hand-held device.

One company has licensed a Strand Displacement Amplification (SDA) method, and has devised an electrical method of binding DNA to silicon chips and performing hybridization. SDA oligonucleotides (probes) are localized to spots on the chip by charge and immobilized on the surface by chemical reaction. The sample is then added to the chip and by applying an electric current, the binding of test to the probes is highly accelerated (one to three minutes). By reversing the charge, unbound molecules are removed and only perfect matches remain. The entire process takes about 15 minutes. Chips for identifying pathogens such as the bacteria responsible for anthrax are under development.

**PCR-based instruments.** The newest technologies in polymerase chain reaction (PCR)-based instruments involve instrument miniaturization and methods for handling and detecting multiple pathogens in multiple samples. The ability to prepare clean PCR templates in a field is often difficult or limited. However, the presence of various chemicals can inhibit the amplification, giving false negative results and, in the case of an attempt to identify a biological threat, possibly endanger people's lives. As a result, a number of companies have started to offer sample preparation units with their PCR instruments.

The advanced nucleic acid analyzer (ANAA), developed in 1997, was the first DNA recognition instrument designed for work in the field. It was portable, but still large and was superseded by a hand-held ANAA (HANAA).

The major differences between the various instruments are in the proprietary heating and cooling systems, detection optics, and sample preparation and handling, as well as size. Speed of most of these instruments is similar with the typical sample analysis taking 7–20 minutes.

A different technology, but still PCR-based, uses a high-performance liquid chromatography to separate the

PCR products and identify mutations. The advantage of the system is that it can detect mutations in any genes that could have been altered for designing biological weapons, thus, potentially complementing any other detection methods.

**Application of DNA recognition instruments.** DNA recognition instruments are likely to be used in general monitoring of the environment, investigation of suspicious objects, and in diagnostics. In all of these applications, detection must be rapid and accurate in order to introduce prevention measures or rapid treatment. Ease of use and result interpretation are important, as in majority of cases, users will be people with minimal laboratory training.

As of 2003, the majority of these advanced DNA recognition instruments were or are undergoing final testing in the field. They are able to cope with samples of water, food, and various clinical samples to detect an environmental contamination or identify a pathogen causing unusual symptoms in humans or domestic animals.

#### ■ FURTHER READING:

##### PERIODICALS:

- Belgrader, P., W. Bennet, D. Hadley, et al. "PCR Detection of Bacteria in Seven Minutes." *Science* no. 5413: 449–450.
- Cao, Y. W. C., R. Jin, C. A. Mirkin. "Nanoparticles with Raman Spectroscopic Fingerprints for DNA and RNA detection." *Science* no. 5586 (2002): 1536–1540.
- Park, S. J, T. A. Taton, and C. A. Mirkin. "Array-Based Electrical Detection of DNA with Nanoparticle Probes." *Science* no. 5559 (2002): 1503–1506.

##### SEE ALSO

*Biosensor Technologies*  
*Bioterrorism, Protective Measures*  
*DNA Sequences, Unique*

---

## DNA Sequences, Unique

---

■ AGNIESZKA LICHANSKA

Deoxyribonucleic acid (DNA) contains genetic information of an organism that is unique for each organism. The entire cellular DNA of any organism, bacteria, plant or animal is known as its genome, as is the entire genetic material of a virus. A DNA sequence is considered to be unique if it is present in only one copy in a haploid genome. A haploid genome contains only a single copy of each chromosome. In humans, for example, a haploid number of chromosomes is 23. However, not all of the DNA contained in the genome is considered as unique; there are also various repetitive sequences present.

## DNA and Genome Structure

A DNA strand is composed of a strand of nucleotides (nitrogen-based building blocks of DNA and RNA). Each nucleotide contains a phosphate attached to a sugar molecule (deoxyribose) and one of four bases, guanine (G), cytosine (C), adenine (A) or thymine (T). It is the arrangement of the bases in a sequence, for example ATTGCCAT, that determines the encoded gene. This sequence allows scientists to identify organisms, genes, or fragments of genes. One of the main characteristics of DNA is the fact that it forms double stranded molecules (helices) by forming hydrogen bonds between the complementary strands inside the helix and a sugar-phosphate backbone outside. This pairing is not random, A always pairs with T, and C pairs with G; therefore, a sequence complementary to ATTCCGAT will be TAAGGCTA.

Genes are the sequences of encoded proteins, and together with the surrounding regulatory sequences are, considered as unique genomic sequences, because they are present as single copies in a haploid genome. In contrast, some sequences are present in multiple copies and are known as repetitive fragments. The simplest genomes of viruses and bacteria contain mostly unique sequences with only a few repetitive regions. However, the proportion of repetitive DNA increases in higher organisms, for example sea urchins have only 38% unique sequences and human just over 50%.

The genes encoding the same protein in bacteria, plants, and humans show some similarity as the majority of the encoded proteins perform the same or similar function across the species. Such homology between the sequences allows scientists to identify the genes in humans by using fragments of mouse or yeast genes to search for similar DNA fragments. Although most of the genes show some species-dependent differences, not all of them can be used to discriminate between organisms. Only a few genes can be used for this purpose. The two main groups are ribosomal (16S in bacteria and 18S in animals) and mitochondrial genes.

Ribosomal genes are useful for tracing evolution and relationships, especially in bacteria. However, mitochondrial genes have an advantage over the ribosomal genes as they are not encoded by the nuclear DNA, but are present as circular molecules in the cells. As such they are less likely to be degraded with time; therefore bones, teeth, or tissue fragments can be identified even after a long time.

## Exploiting Unique DNA Sequences

The presence of unique DNA sequences allows scientists to identify signature sequences that can be later used as probes to detect individual organisms or to detect a particular gene. Changes of even one base pair can be readily detected by most hybridization techniques and by

sequencing. Signature sequences are particularly important for diagnosis of viruses, which are the pathogens that lack ribosomal or mitochondrial genes. Their detection and identification is greatly simplified by using these sequences, as traditional methods can take up to a few weeks.

The unique DNA sequences can also be used to design primers (short DNA fragments needed to initiate DNA amplification) for polymerase chain reaction (PCR). There is adequate difference between all the genes within one organism, as well as between organisms from different species, to ensure that the selected primers will only amplify the target sequence even if a mixture of different DNA molecules is present. This allows scientists to design diagnostic and identification tests for the common pathogens and diseases and for parts of the pathogen's genome.

**Identification of people.** Although every person has unique DNA (except for the identical twins), identification of people is not based on the sequencing of someone's genome. Instead, analysis of mitochondrial DNA in a region of a displacement-loop (D-loop or control region) or of short tandem repeats (STRs) is used for identification purposes. D-loop analysis is used for individual identification in forensic analysis. This is possible due to the polymorphisms of such sequences resulting from substitutions of base pairs during DNA replication process (for example, instead of A, DNA polymerase incorporates T).

The D-loop region is 1274 base pairs long and is located between the genes encoding transfer RNA (tRNA) for proline and tRNA for phenylalanine and contains the regulatory regions of the for replication other genes.

The main method used for the identification of the changes in this region is PCR amplification and sequencing. However, new microarray approaches are under development.

**Encoding secret messages.** DNA sequences offer a unique method of encrypting messages or concealing information. A DNA sequence encoding a message is flanked on the sites by primers that will be later used to amplify if by PCR and sequence. An encryption code is selected by a group that is using the system; for example, each letter and number might be assigned three base pairs. The DNA strand with a message is prepared and mixed with human genomic DNA fractionated to the same size as the message. To further conceal the DNA from an enemy, DNA from another species can be added. An intended recipient of the message can decode it by PCR amplification and sequencing. Sending such as message is as simple as writing a letter and enclosing the DNA coded message as a microdot. Once the DNA mix is prepared, it is spotted over a dot on paper from which the microdots are cut out and attached to the full stops in the letter. If such a letter falls



into the wrong hands finding a message will be extremely difficult, as it will be buried among millions of others, and reading it without the primer sequences and encryption code will be impossible.

DNA encrypted messages can be used for safekeeping important information, but also to pass on espionage information. Although the method is simple, it requires molecular biology equipment to decode and can be too troublesome for everyday use.

## Use of Unique DNA Sequences

Unique DNA sequences are already used as security tools. The ability to synthetically create DNA molecules allows the generation not only of spy messages, but more importantly, unique signatures that would protect consumers from product fakes. Similar methods were used at the Sydney Olympic Games in 2000 to mark all of the official merchandise. In this case, an invisible ink mixed with DNA obtained from one of the athletes was used. Protection is not limited to manufacturers. Unique DNA sequences are also used by artists such as Thomas Kinkade and cartoon creator Joseph Barbera, who protect their artwork by DNA signatures.

The major use of unique DNA sequences for security, however, is in the area of environmental surveillance and identification of agents of biological warfare. The sequences used for these purposes are often kept secret. Most of the producers of DNA recognition instruments use such sequences to design their products.

Finally, forensic science relies in many cases on the use of unique sequences for identification of biological traces and individual identification.

### ■ FURTHER READING:

#### BOOKS:

Strachan, Tom, and Andrew P. Read. *Human Molecular Genetics*, 2nd ed. Oxford: BIOS Scientific Publishers, 1999.

Hartl, Daniel L. *Genetics*. Boston: Jones and Bartlett, 1994.

#### PERIODICALS:

Clelland, C. T., V. Risca, and C. Bancroft. "Hiding Messages in DNA Microdots." *Nature* no. 6736 (1999): 533–534.

#### ELECTRONIC:

Wired News. "DNA Tagging." Stewart Taggart. <<http://www.wired.com/news/print/0,1294,34774,00.html>> (15 January 2003).

#### SEE ALSO

*DNA Fingerprinting*  
*DNA Recognition Instruments*  
*Polymerase Chain Reaction (PCR)*

## DNA Technology.

SEE *Genetic Technology*.

## Document Destruction

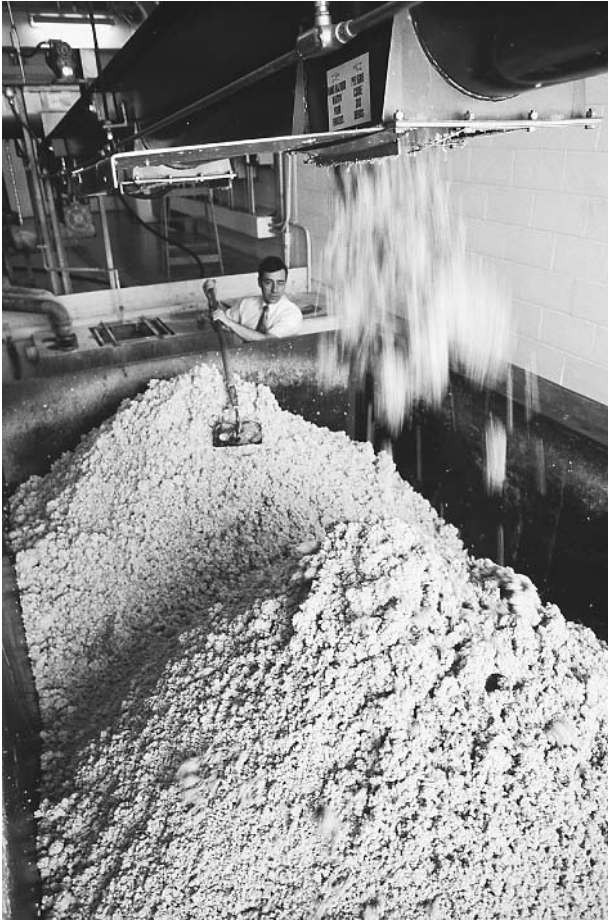
■ JUDSON KNIGHT

Modern society that has become so accustomed to the digitization of data may forget just how much information remains available in physical format. Even documents stored on a computer may circulate as hard copy, and these, combined with other paper items such as phone messages, notes, memoranda, and other items provide an opportunity for the theft of useful information. Businesses targeted for economic espionage are particularly vulnerable, as are individuals, either due to their own carelessness or that of companies charged with maintaining sensitive records. For that reason, businesses have increasingly turned to document destruction, a security solution long applied by government agencies. Document destruction can be achieved with shredders, burn boxes, and other forms of technology, often in industrial facilities dedicated to that purpose.

Stories of document destruction by businesses and public officials regularly appear in the media. In 2002, as a scandal erupted around Enron Corporation for falsifying records of earnings, it was revealed that Arthur Andersen LLP, the accounting firm that had helped Enron falsify its books, had shredded literally tons of documents.

Other businesses employ document destruction for much more legitimate reasons, such as protection against economic espionage. But not only businesses need to destroy documents; so do individuals. According to the United States Postal Service, half a million people each year become victims of identity theft, which occurs when a criminal steals financial information from someone, then poses as that person in order to siphon off funds. One of the most significant avenues of vulnerability in this area is the household trash. A person may receive an unsolicited credit card offer and, dismissing it as junk mail, throw it away. Once garbage is placed on the curb for pickup, it is easy for a thief to pick through it, remove the credit card offer, fill it out, send it in, and obtain a "free" card—all courtesy of an innocent consumer who failed to take appropriate precautionary measures.

In the 1990s, these garbage-combing thieves earned the colorful appellation of "dumpster diver". Private detectives, for purposes either laudatory or malign, also obtain a great deal of their information from trash. (So, too, do law-enforcement officers, who take advantage of the fact that material an individual has discarded is open to search without a warrant.) Yet not every aspect of



SOMAT (soluble materials), or shredded documents, are loaded into disposal bins at C.I.A. headquarters in Virginia. ©ROGER RESSMEYER/CORBIS.

individual vulnerability to identity theft or invasion of privacy involves those intent on misusing individuals' private records.

## Forms of Document Destruction

The best methods of document destruction take place on an industrial scale. The document destruction industry, which primarily serves corporate clients, is estimated to generate \$1.5 billion a year in revenue. Whereas only about two dozen companies nationwide were in operation in the early 1980s, by 2002 that number had risen to about 600.

Document shredding, which particularly came to national attention in the wake of the Enron debacle, is only one of many methods of document destruction, though it is the one most frequently used. As a report in the *Wall Street Journal* noted, "For routine destruction work, many companies use shredding services because even heavy-duty office-model shredders tend to choke on anything thicker than about 50 pages—and can be stopped dead in their tracks by a binder clip."

**Industrial shredders.** By contrast, the shredders at a facility such as that of American Document Security Corporation (ADS) in Brooklyn, New York, are capable of chewing through 20 tons (18.14 tonnes) of documents an hour. Clients of such companies range from law and consulting firms to investment banks, hospitals, and many others.

Though document shredding is probably as old as the concept of written documents, shredding by machine dates back to the 1920s, when an American inventor developed the first shredder from a Bavarian noodle cutter. Today's shredders are far more efficient than those used even in 1979, when the students who took over the U.S. embassy in Teheran, Iran, were able to piece together documents shredded by embassy personnel.

Some shredders are known as disintegrators. Often used for destroying CD ROMs, circuit boards, and other items containing computerized data, these chop up materials into a fine dust that can be sifted through a screen at the bottom of the machine. Another variation on the shredder, inasmuch as it destroys documents by purely physical (rather than chemical or electromagnetic) means, is a hammer-and-mill device, which beats paper quite literally to a pulp.

**Burning and other methods.** Paper that has been put through industrial shredders and hammer-and-mill devices often is recycled. Waste-to-energy plants burn paper waste at temperatures as high as 2,200° F ( 1,204 °C).

For burning documents on a smaller scale—especially documents for which security is an extremely high concern—a burn box may be used. Actually, the purpose of the burn box is not to destroy documents per se, but to destroy documents discovered by the wrong people. Inside the box, a sturdy metal container, is a volatile chemical mixture attached to a tamper-sensitive switch. If someone opens the box in an unauthorized manner, the chemicals turn the pages to ash.

**A focus on security.** An intriguing variety of document destruction can be used for electronic media such as CD-ROMs, hard drives, floppies, and so on. This is a degausser, which applies electromagnetic energy to rearrange particles of information. Used either in the form of a stationary box or a hand-held wand, a degausser removes information permanently, leaving the storage device free to be used again.

No matter how advanced the technology, however, it is only as reliable as the individual who operates it. For this reason, security concerns are as much a motivator to document-destruction companies as they are to the firms who hire them. ADS, for instance, equips its trucks with alarms, and tracks them on a global positioning system to ensure that documents are not stolen en route. Its employees are bonded, and must undergo background checks prior to employment. Some 30 security cameras are in

operation at the Brooklyn facility. Similarly, at the trash-to-energy facility in Utah, a closed circuit television system, along with security guards, provides surveillance during the unloading and burning process.

## ■ FURTHER READING:

### PERIODICALS:

- Brown, Ken. "When Enron Auditors Were on a Tear." *Wall Street Journal*. (March 21, 2002): C1.
- Choi, Audrey. "VW Discloses GM Documents Were Destroyed—German Car Maker Denies Involvement, But Rival Still Claims Espionage." *Wall Street Journal*. (August 9, 1993): A3.
- "Document Destruction." *Government Executive* 30, no. 8 (August 1998): 58.
- Eichenwald, Kurt. "Andersen Charged with Obstruction in Enron Inquiry." *New York Times*. (March 15, 2002): A1.
- Kirch, John F. "Document Destruction." *Security Management* 42, no. 8 (August 1998): 22–23.
- Orey, Michael. "Why We Now Need a National Association for Data Destruction." *Wall Street Journal*. (January 30, 2002): A1.
- Rowh, Mark. "Shredders: The Cutting Edge." *Office Solutions* 19, no. 8 (September/October 2002): 42–44.

### ELECTRONIC:

- National Association for Information Destruction. <<http://www.naidonline.org>> (March 30, 2003).
- Trujillo, Al. "Avoid Risk with Secure Document Destruction." *Electronic and Hardcopy Document Processing Technology*. December 2002. <<http://www.dptmag.com/editorial2.asp?ID=97>> (March 30, 2003).

### SEE ALSO

*Computer and Electronic Data, Destruction*  
*Economic Espionage*  
*Privacy: Legal and Ethical Issues*

## Document Forgery

### ■ MARTIN J. MANNING

The use of forgeries to deceive an enemy or affect public opinion has been a staple of disinformation throughout modern history. Forgeries can be more easily exposed than other types of active deception measures largely because careful analysis can often demonstrate convincingly that the documents are fraudulent. Still, forgery is effective in at least three ways. First, a forgery can cast aspirations on targeted governments and on individuals (silent forgery). This can be the most damaging forgery, as the victim does not know that the forgery is being circulated and may never get the opportunity to refute it. Second, forgeries, when publicized, force the target government to spend time, effort, and funds on refutation.

Third, denial never entirely offsets the damage done as doubt can be cast by repeated reference to the forgery and to its contents.

**Cadore letter.** On August 5, 1810, Jean, Duc de Cadore, a French foreign minister, delivered a diplomatic note to the United States minister John Armstrong. In it, Napoleon I promised to revoke the Berlin and Milan Decrees in November, 1810, if the British Orders-in-Council were repealed, or if the United States reinstated sanctions against Great Britain. The latter happened and non-intercourse against the British resumed on February 28, 1811. The Cadore letter turned out to be a forgery. American ships continued to be sized and President James Madison refused to change his decision with regard to the British embargo.

**De Lome letter.** Written by the Spanish minister to the U.S., Enrique de Lome, to a friend in Havana, the letter was published in William Randolph Hearst's *New York Journal* in February, 1898. It characterized President William McKinley as "weak and a bidder for the admiration of the crowd" and questioned McKinley's political integrity. This private letter was stolen by a Cuban rebel sympathizer from the Havana mail system and returned to New York. The publication of the letter uncovered the false promise of Spain's foreign policy towards the U.S. In its wake, De Lome immediately resigned, Spain sent an insincere apology, and McKinley let the incident pass, although it ignited American opinion toward future Cuban intervention.

"Protocols of the Learned Elders of Zion." No country, however, has used forgeries as extensively as the Soviet Union, developing forgeries to a level unparalleled in previous times. For the Soviets, forgeries were a weapon of active measures (i.e., influence operations) that supported propaganda themes. The KGB had the responsibility for carrying out active measures and producing forgeries. Describing the role of the KGB in influencing attitudes in the West, Yuri Andropov, then head of KGB, said in 1967, "The state security bodies are also actively participating in the fulfillment of this task. The workers of these bodies are aware that peaceful coexistence is a form of class struggle; that it is a bitter and stubborn battle on all fronts, economic, political, and ideological. In this fight, the state security bodies are obliged to carry out their specific duties efficiently and faultlessly." These Soviet state security bodies built upon the activities of the czarist secret police (Okhrana,) who produced one of history's classic forgeries.

Among the most widely circulated propaganda tracts and the centerpiece of anti-Semitic literature, the infamous "Protocols of the Learned Elders of Zion" appeared shortly before the 1905 uprising against the Czar Nicholas II of Russia. It was authorized by Pyotr Ivanovich Ratchkovski, the head of the Okhrana, who circulated it, although authorship is now given to Mathieu Golovinski. The forgery derived from a French political pamphlet,



**Forged passport** with picture of himself in disguise enabled Lenin to escape to Finland in the fall of 1917. Warrant for his arrest had been issued in July of that same year.

This false passport and disguise enabled Lenin to escape into Finland after an order for his arrest was issued by the Russian Provisional Government in July 1917. ©HULTON-DEUTSCH COLLECTION/CORBIS.

"Dialogue aux Enfers entre Montesquieu et Machiavel," by Maurice Joly, which was first published in 1864 as an attack on Napoleon III's ambitions for world domination. In the "Protocols," "the Jewish," or "the Jews," were substituted where the French emperor was mentioned in the text.

The Okhrana, was responsible for the "Protocols," a forgery that cost untold number of lives since it was first introduced. The Nazis used this forgery as a justification for genocide against Jewish persons, and even today anti-Semitic groups continue to reprint it.

**German-Bolshevik conspiracy.** Drawing on the experience of their Czarist predecessors, the Soviet KGB (known earlier as the Cheka, OGPU and GPU) continued to use forgeries. Six months after seizing power, the Bolsheviks were concerned about continuing accusations labeling Lenin and his comrades as German agents. There was some logic to this accusation, as the Germans had helped send Lenin back into Russia to undermine their wartime enemy. The Bolsheviks denied that they were in the pay of the Germans. On September 15, 1918, the United States government released to the press a collection of documents that

purported to show that the Bolsheviks had received money both before and after the Russian Revolution. In October, 1918, the Committee on Public Information (CPI), the World War I predecessor of USIA, released a pamphlet to the press entitled "The German-Bolshevik Conspiracy" which contained translations of 68 documents and reproductions of many of them. In addition, the pamphlet contained an analysis of the documents prepared for the National Board for Historical Service by two distinguished scholars. The report concluded that most of the documents were genuine, although some were questioned. The documents had been obtained in Russia by Edgar Sisson, the CPI representative, and came to be known as the "Sisson documents."

The release of the Sisson documents was reported in the American press on September 16, 1918, but, on September 21, the *New York Evening Post* challenged their authenticity, citing as their source Santeri Nuorteva, who was described by them as "head of the Finnish Information Bureau in New York," a notorious Soviet propagandist who had been a representative of the short-lived Communist government established in Finland by the Red Army. Nuorteva revealed that the first American to see the documents was Col. Raymond Robins, the Red Cross administrator in Russia who was later identified as a Bolshevik sympathizer.

The controversial Sisson documents are consistent with documents proving German financing of the Bolsheviks that were found in the German Foreign Office after World War II. The possibility exists that the Bolsheviks created a set of forgeries which were then mixed with authentic documents, and passed to the American government by Robins for the purpose of discrediting the thesis that Lenin and company were on the German payroll. In fact, the exposure of the Sisson documents created an atmosphere in which any allegation of German financial support to the Bolshevik was treated with distrust. It was only decades later that the German Foreign Office documents became available and proved the point.

**Zinoviev letter.** On October 25, 1924, the British Foreign Office released to the press the text of an alleged document of the Communist International ordering the British Communist Party to carry out activities against the Labour government and to organize cells in the army. The document signed with the name of the head of the Communist International, Grigory Zinoviev, is credited with bringing down the British Labour government, which was perceived as being too soft on the Soviet Union.

The Soviet government and Zinoviev denied the authenticity of the letter. However, it was quite consistent with instructions given to the British and other Communist parties by the Fifth World Congress of the Communist International held in Moscow in the summer of 1924. The instructions had been printed in the September 5, 1924 issue of the official Comintern publication, *International*

*Press Correspondence*, published in German and English in Vienna.

**Tanaka memorandum.** In 1929, a different form of Soviet forgery appeared when a document, purporting to be a memorandum from the Japanese Prime Minister Tanaka to the Emperor Hirohito, found its way into the Western press. This document laid out a Japanese plan for world conquest. According to the introduction to a 1941 publication of the document by the American Communist Party, "The Tanaka Memorial...was written in 1927 as a confidential document. It first came to light in 1929 after it had been purchased from a Japanese by Chang Hsueh-liang, then the Young Marshal of Manchuria," a warlord who frequently collaborated with the Chinese Communists. In late 1936, he kidnapped Chiang Kai-shek and demanded that he cooperate with the Communists in the war against Japan.

The Tanaka document was clearly a forgery. It contained errors of fact about Japan and even about Baron Tanaka, but it was widely circulated until the end of World War II. An insight into its Soviet origin was provided in 1941 by Leon Trotsky, who argued that it was authentic. According to an article by Trotsky, written shortly before his death, Felix Dzerzhinsky, the head of Cheka, secured the document in 1925 through a spy in the Japanese Ministry of Foreign Affairs. The document was photographed and then translated for Trotsky. Trotsky did not explain how the Soviets came into possession in 1925 of a document not written until 1927, the year Tanaka became prime minister. It is possible that the Soviets created the forgery based on an authentic document stolen in 1925.

Trotsky revealed that the document was put into circulation in the United States through Amtorg, the Soviet trading corporation, headed by man named Bogdanov. Since Bogdanov did not arrive in the United States until 1930, Trotsky's knowledge of the method of surfacing could only have come through his contacts in the GPU, which he maintained after being ousted from the Soviet leadership. This date would be consistent with the forgery's original surfacing in China in 1929 and its replay in the United States in 1930.

The most recent replay of the Tanaka forgery was a reference to it in a Kuwaiti newspaper in January, 1987. The unsigned article, in Arabic, which showed substantial evidence of Soviet authorship, accused the United States of developing an "ethnic weapon," a biological weapon that would supposedly affect only black or brown skinned people. This bizarre allegation has been repeated in both official Soviet media and in publications influenced by the Soviets for years. The article was also accompanied by a purported picture of the "ethnic weapon" being fired and carried the caption, "The germ bomb is fired from regular tanks looking like regular bombs and spreading the germs." The opening paragraphs of the article accused the United States of taking over biological weapons research from

the Japanese, who were supposedly carrying out the plans revealed by Tanaka in his letter to the Emperor.

**Whalen documents.** In 1930, the U.S. Congress was planning to establish a committee to investigate Communist propaganda. Shortly before it was formed, the New York City police department received copies of a set of documents purporting to be letters from the Communist International instructing Amtorg to carry out Communist propaganda in the United States. Amtorg actually was deeply involved in Soviet espionage in the United States. The documents were released to the press on May 2, 1930, and appeared in print the next day. They were released by police Commissioner Grover Whalen and came to be known as the "Whalen documents."

An examination of the documents revealed that they were forgeries. For example, the letterhead read "Isполком Коминтерна" (Excom Comintern). An authentic document would have spelled out "Communist International," rather than using the nickname Comintern. The forgeries were exposed by journalist John L. Spivak, who provided the evidence to Congressman LaGuardia and wrote about the case in the *New York Evening Graphic*.

Spivak claimed that his editor gave him the assignment to trace the documents on May 3. After investigating type foundries and print shops, he said he discovered the identity of the printer of the letterheads on May 8. It took him four days to trace the printing. Spivak's story does not stand up to investigation. When the printer testified before a congressional committee, he revealed that he recognized the letterhead when he saw it reprinted on the front page of the Yiddish language daily newspaper, *The Jewish Daily Forward*. The same day, Spivak came into his store and accused him of being the printer of the letterheads. The printer Max Wagner, signed an affidavit for Spivak acknowledging that he had the printed the letterheads. The statement, read into the *Congressional Record* by Congressman Fiorello LaGuardia, states, "I printed this about four months ago and submitted two copies as a proof, but the man did not come back for the order, Signed, M. Wagner, printer."

The photostat of the letterheads appeared on the front page of *The Jewish Daily Forward* (May 3, 1930), the date that Spivak began his investigation, not four days later. It is clear that Spivak knew the printer's identity as soon as he began his investigation.

The Communist Party newspaper, *Daily Worker* (May 13, 1930) reproduced a photostat of the Wagner affidavit with a slightly different text leaving out the word "printer" and inserting the words "May 8, 1930." This appears to have been concocted to authenticate Spivak's claim that he confronted Wagner on May 8th rather than on May 3, when the incident actually took place.

In 1945, Elizabeth Bentley revealed to the FBI that she had worked as courier for a Soviet spy ring and she identified Spivak as a member of the ring. The Communists used the forgeries to discredit the congressional

committee established to investigate Communist propaganda. The committee, headed by Congressman Hamilton Fish of New York, never authenticated the Whalen documents. However, Earl Browder, then head of the Communist Party U.S.A., reported to a meeting of the Executive Committee of the Communist International held in Moscow in April, 1931, that, "the notorious forged 'Whalen Documents,' produced by the Czarist 'General' Djamgaroff, became the occasion for the U.S. Congress to set up the Fish Committee to investigate Communist activities in the U.S. Behind the actions of this committee, which were the most vulgar farce considered in themselves, was the sinister and serious purpose of preparing 'public opinion' for the war of intervention against the U.S.S.R." Badacht was later revealed, by Whittaker Chambers, as the man who recruited him as a Soviet spy. Badacht was the contact between the leadership of the American Communist Party and the Soviet intelligence service.

**Other events.** Since World War II, the Soviet Union continued to release forgeries that it expected would damage U.S. relations with its allies. Several were important campaigns. One was designated the Eisenhower-Rockefeller Letter, an extensive forgery presented as a private "letter" from Nelson A. Rockefeller to President Dwight D. Eisenhower in which Rockefeller was portrayed as the advocate of a "bolder program of aid to under-developed countries," as a cover for what the East Germany press called "supercolonialism" ("superkolonialismus"). Its aim was to discredit the U.S. commitment to the removal of the old colonial powers from their involvements in Africa and in Asia.

The document first appeared on February 15, 1957, in the East German daily, *Neues Deutschland*, and circulated throughout the world during what was termed the "Camp David" period of East-West cordiality (1959–1960); it later appeared on Radio Moscow, in *Pravda* (Soviet party newspaper), on Radio Hanoi, on Radio Beijing, in the Czechoslovak domestic press, and in the official news agency of the People's Republic of China.

In 1961, Richard Helms, assistant director of the Central Intelligence Agency, testified before the U.S. Senate. He said, "Long before 1957, the Communists were as skillful as the Nazis in the production and exploitation of forgeries. But in that year, they first began to aim them frequently against American targets, to turn them out in volume, and to exploit them through a wide-flung international network. Then CIA put these fakes under the microscope. We found that each Soviet forgery is manufactured and spread according to a plan. Each is devised and timed to mesh with other techniques of psychological warfare in support of Soviet strategy." During this period, more than 32 forged documents were found.

In a 1980 report to the U.S. Congress, the CIA revealed that "the KGB provides a non-attributable adjunct to the overt Soviet propaganda network. Service A of the KGB's

Foreign Intelligence Directorate plans, coordinates and supports operations which are designed to backstop overt Soviet propaganda using such devices of covert actions as forgeries, planted press articles, planted rumors, and controlled information media. In particular, the number of Soviet forgeries has increased dramatically in recent years. In the early 1970s, this section of the KGB was upgraded from "department" to "service" status—an indication of its increased importance. Service A maintains liaison with its counterparts in the Cuban and the East European services and coordinates its overall program with theirs."

The "U.S. Army Field Manual, FM 30-31B," also known as "Stability Operations-Intelligence," was the most ubiquitous forgery of recent years. In September, 1976, a photocopy of this forgery appeared on the bulletin board of the Philippine Embassy in Thailand, together with a letter addressed to Philippine President Marcos. The forgery said that the United States planned to use leftist terrorist groups in Western countries to promote U.S. objectives. It reappeared in 1978 in two Spanish publications where it had been planted by a Spanish Communist and a Cuban intelligence officer. The next year, copies of a Portuguese language translation were circulated by the Soviets among military officers in Lisbon.

The forged field manual had worldwide distribution in the late 1970s. In January, 1979, *Covert Action Information Bulletin*, published in the United States by CIA defector Philip Agee, reproduced the forgery as if it were an authentic document. While the original forgery was a typescript, the magazine reset it in font that gave the impression that it was a printed document.

In 1983, the Soviets began to replay the story. In the new version, the manual had been discovered in the possession of the Italian Masonic organization P2, which was involved in an important scandal at the time. This was an attempt both to link the United States government to the scandal and to authenticate the forgery.

**Presidential review memorandum on Africa.** On September 17, 1980, White House press spokesman Jody Powell announced that an unidentified group had sought to sow racial discord by circulating a forged presidential review memorandum on Africa that suggested a racist policy on the part of the United States. The first surfacing on the forgery appears to have been in the San Francisco newspaper, *Sun Reporter* (September 18, 1980). The *Sun Reporter's* political editor, Edith Austin, claims in that issue of the paper to have received the document from an "African official on her recent visit on the continent." The forgery was replayed by the Soviet news agency TASS on September 18, 1980, and distributed worldwide.

**Kirkpatrick speech.** Former United States ambassador to the United Nations Jeanne Kirkpatrick has been the target of more than one Soviet forgery. On February 6, 1983, the pro-Soviet Indian weekly, *Link* published the text of a

supposed speech by U.N. Ambassador Kirkpatrick outlining a plan for the Balkanization of India. The speech was never given, but this forgery has been replayed many times by Soviet-controlled propaganda outlets. Its most recent appearance was in the book, *Devil and His Dart*, published in 1986. The author, Kunhanandan Nair, was the European correspondent of *Blitz*, another pro-Soviet publication.

On November 5, 1982, the British magazine, *New Statesman* published a photostat of a letter supposedly from a South African official to Kirkpatrick. He was allegedly sending her a birthday gift. The U.S. Mission to the U.N. wrote the magazine on November 19, branding the letter a forgery. *New Statesman* countered this by printing another photostat of the forgery with entirely different spacing between the lines. The magazine claimed that the letter was authentic and that they had received it from a source in the U.S. Department of State. A comparison of this forgery with a letter sent by the South Africa official to a number of U.S. journalists announcing his appointment as information counselor at the embassy revealed that this letter was the exemplar. The real letter had been typed on a computer. The forgery based on it was typed on a typewriter and contained a number of misspellings.

**Los Angeles Olympics forgery.** In the summer of 1984, two bizarre leaflets were mailed to African and Asian participants in the Los Angeles Olympics, which were boycotted by the Soviets. Signed by the Klu Klux Klan, they threatened the lives of these athletes. These leaflets later proved to be Soviet forgeries, written in poor English. When the U.S. government exposed them and pointed out that there is no organization in the United States called simply the Klu Klux Klan (the organizations bear individual names like White Knights of the Klu Klux Klan or Invisible Empire of the Klu Klux Klan), TASS, the Soviet official news agency, responded on July 12, 1984, by claiming that the leaflets were signed "the Invisible Empire, The Knights of the Klu Klux Klan." TASS attempted unsuccessfully to correct the error on the leaflets made by the KGB. The forgeries were intended to preoccupy African-American and Asian-American athletes with intimidation, and negatively affect their performance. Despite the lack of Soviet competition, Americans won a record 83 gold medals at the 1984 Olympics, led by the 23-year-old African-American Carl Lewis.

**Weinberger speech and the Strategic Defense Initiative.** During the summer of 1986, West European journalists received a copy of the text of a supposed speech by U.S. Secretary of Defense Casper Weinberger on the Strategic Defense Initiative (SDI). No such speech was ever made. The forgery contained five falsehoods: first, that the U.S. had a desire for military "prevalence" (superiority) over the Soviet Union in order to be able to achieve victory in a "controlled nuclear exchange" (limited nuclear war) or a protracted war; second, that the United States would use

SDI to "prevent the development of unfavorable tendencies" in NATO and to control its allies was false; third, that SDI would enable the U.S. "to threaten the Soviet Union with a knock-out blow"; fourth, that SDI would "coerce the Soviet Union and make a practical contribution to the liberation of all nations enslaved by Communist totalitarianism, including, possibly, even the Russians themselves" were false; fifth, that SDI would enable the U.S. to maintain a technological lead over its "rivals" in the free world; and sixth, that the Soviets do not have their own form of SDI were additional false statements. The Weinberger forgery was intended to assist the Soviet active measures campaign. However, it was exposed by the U.S. government and did not serve Soviet purposes.

**The Schweitzer-Pinochet letter.** In July 1985, an Italian journalist found a copy of a letter signed with the name of General Robert Schweitzer, the head of the Inter-American Defense Board. The letter was a forgery addressed to President Pinochet of Chile asking him to provide troops to fight on behalf of the United States in Central America. The journalist contacted the U.S. Embassy and within the day received evidence that the letter was a forgery. He did not write a story based on the letter. A few days later, however, another Italian press service ran a story datelined Mexico City based on the letter. When they were advised it was a forgery, they investigated and discovered that the letter had been provided to one of their writers by the public relations man for the Guatemalan insurgency, which was supported by Cuba and Nicaragua. The news service ran an expose of the forgery, attributing it to the Cubans and Nicaraguans. This incident points to a problem the Soviets had in surfacing forgeries. On the one hand, the common technique of using a plain, unmarked envelope to surface the forgery creates suspicion in the mind of the recipient. On the other hand, the use of a human being to pass on the forgery provided a trail leading back to the forger.

Former United States Information Agency (USIA) specialist in Soviet disinformation Herbert Romerstein wrote a letter to General Schweitzer on August 16, 1985, providing background on the forgery, then sent a copy of this letter to the U.S. Senate Committee on Foreign Relations, where he testified, for printing in a Congressional report on Soviet active measures. Romerstein wrote the word "copy" on the top of the letter then, at the request of a Czech diplomat, Vaclav Zluva, provided him with a copy of this letter. As a precaution, Romerstein drew a line under the word "copy" on the original from which all subsequent copies were made, which made Zluva's letter unique and identifiable.

In August 1986, the *Washington Post* and *U.S. News and World Report* received a forgery in a plain white envelope signed with Romerstein's name. The *Washington Post* called him in; he looked at it, explained the forgery, and the newspaper carried a story on it (August 19, 1986). The forgery was on the letterhead of the United States Information Agency and was signed with

Romerstein's name. At the top of the forgery was the word "copy" with no line under it. This made it clear that the exemplar for the forgery was the letter Romerstein had given to the Czech. When Romerstein confronted Zluva about this, he admitted sending the exemplar to Prague.

In the forgery, Romerstein made it appear as if he had organized a USIA effort to spread all of the false stories that had appeared around the world after the Chernobyl disaster. In fact, the false stories were generated by Soviet reluctance to reveal information about the accident. On April 26, 1987, the Soviet publication *Moscow News* admitted, "The formulation, not for the press, is being used more and more often. Why cannot our press use what is being regularly reported to the International Atomic Energy Agency? There are some who do not understand that rumours and hearsay are generated not by summaries and figures, but by their absence."

**Reagan signature.** In the 1980s, before the downfall of the Berlin Wall in 1989 and the Soviet Union in 1991, President Ronald Reagan's signature appeared on a number of forgeries. The last to appear was in May 1987. It was a supposed memorandum to the secretaries of state and defense, and the director of the CIA. In this forgery, which bore the date March 10, 1983, the president was supposedly ordering the establishment of a U.S. military force called the "Permanent Peace Forces" to intervene in Latin America. This forgery received wide circulation in Latin America and was designed to inflame nationalist and anti-American feelings.

The usual path of a Soviet forgery was from the KGB to a target newspaper. When the target was a legitimate publication it became difficult for the Soviets to succeed in planting the forgery. They often used publications which they could control or influence for the initial surfacing. One publication frequently used this way was the Indian newspaper, *Patriot*. In testimony before a British court on March 24, 1987, Ilya Dzhirkvelov, a former officer of the KGB, revealed that in 1962, on KGB orders, he participated in setting up this newspaper.

After a forgery appeared in a publication such as the *Patriot*, it was replayed by the Soviet press agencies TASS or Novosti. This provided copies in every language for KGB officers to plant in the world press through their agents but not all forgeries were meant for publication. They were passed by KGB agents of influence to officials of a target government in the hope that they would believe forgeries designed to increase anti-American feeling. Such forgeries were often unknown to American officials, who had no opportunity to refute many of them. With the fall of the Soviet Union and the relaxation of the American-Soviet rivalry, KGB forgeries lessened, but forgeries continue to remain a significant weapon of disinformation stories worldwide.

**Acknowledgement.** The author wishes to thank Herbert Romerstein, former coordinator of Programs to Counter



Soviet Active Measures, United States Information Agency, for his assistance in compiling this essay, especially in clarifying the different Soviet forgeries. Mr. Romerstein's paper, "Forgeries: A Weapon of Soviet Active Measures," prepared for the 1987 Conference on Soviet Active Measures and Propaganda in the Gorbachev Era: Analysis and Response" should be considered a primary source on the subject. I am grateful to Mr. Romerstein for permission to use this paper and for his helpful comments.

#### ■ FURTHER READING:

##### BOOKS:

- Baldwin, Neil. *Henry Ford and the Jews: The Mass Production of Hate*. New York: Public Affairs, 2001.
- Daugherty, William E. *Psychological Warfare Casebook*. In collaboration with Morris Janowitz. Baltimore, MD: Published for Operations Research Office, Baltimore: Johns Hopkins University by Johns Hopkins Press, 1959.
- Segal, Benjamin W. *A Lie and a Libel: A History of the Protocols of the Elders of Zion*. [Translation by Richard S. Levy of 1926 edition] Lincoln, NE: University of Nebraska, 1995.
- U.S. Department of State. *Active Measures: A Report on the Substance and Process of Anti-U.S. Disinformation and Propaganda Campaigns*. Washington: The Department, 1896.
- . *Soviet Influence Activities: A Report on Active Measures and Propaganda, 1987–1988*. Washington: The Department, 1989.
- U.S. International Communication Agency. *Forgeries of U.S. Documents*. Prepared by the European Branch, Office of Research. Washington: The Agency, 1982.

##### SEE ALSO

*Disinformation  
Propaganda, Uses and Psychology*

## DOD (United States Department of Defense)

#### ■ JUDSON KNIGHT

Although it originated only in 1947, the United States Department of Defense (DOD) comprises elements that date back to the Revolutionary War. Some 3.2 million people, including active military, reservists, National Guard, and civilian personnel, work for DOD, making it one of the nation's largest employers. DOD manages some 600,000 individual buildings or structures worldwide, the most notable of which is the vast five-sided structure in Washington, D.C., whose name is sometimes used to designate the Department as a whole: the Pentagon. Led by the president, as commander-in-chief of the armed forces,

with the advice of the secretary of defense and the National Security Council (NSC), DOD is made up of the military services and the unified commands, whose deployment is coordinated by the Joint Chiefs of Staff (JCS).

### Historical Background

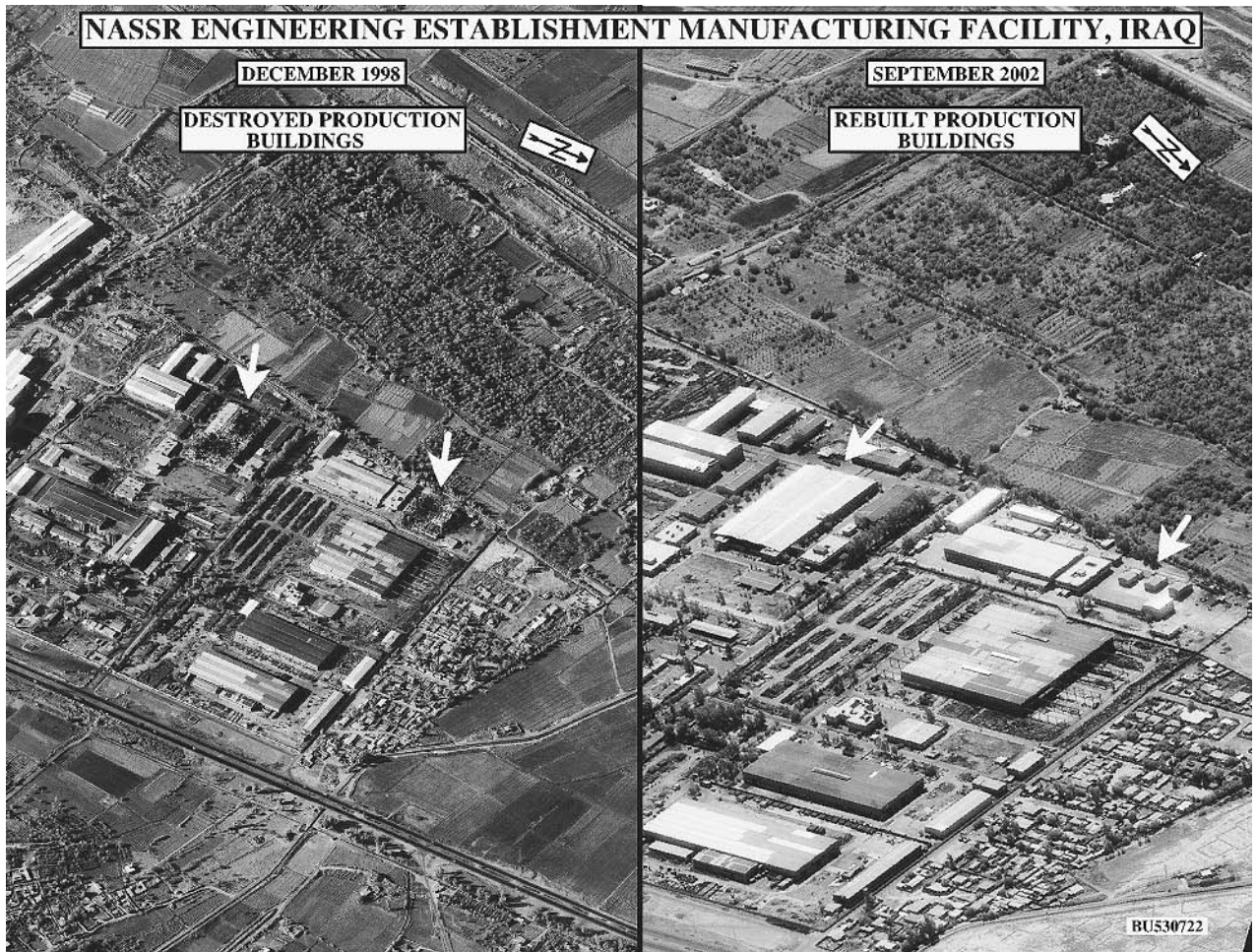
The roots of DOD lie in the establishment of the Army, Navy, and Marine Corps in 1775, at the outset of the American Revolution. In 1789, the new federal government created the War Department, and in 1798 the Department of the Navy, which also includes the Marine Corps. Both the War Department, today known as the Department of the Army, and the Department of the Navy remained Cabinet-level executive departments until 1947.

Another military service, and the only one under DOD control during peacetime, had its roots in the formation of the Revenue Cutter Service in 1790. By 1915, this would become the U.S. Coast Guard, which is today part of the Department of Homeland Security, except in wartime, when it is assigned to DOD. Finally, the U.S. Air Force—which is centered on technology of which the nation's founders could not have conceived—began life as an element of the Army. In 1947, it became a service in its own right.

The statutory foundation of the modern DOD, along with much of the national security apparatus, is the National Security Act of 1947. It created a civilian secretary of defense position, along with a Department of the Air Force. The act transformed the War Department into the Department of the Army, and placed the three major services—Army, Navy, and Air Force—under the secretary of defense. An amendment to the act in 1949 officially created the Department of Defense itself.

**The Pentagon.** Six years before the National Security Act, just prior to U.S. entry into World War II, the War Department built the structure that today symbolizes DOD: the Pentagon. Prior to its construction, War and Navy department operations were housed in some 17 buildings. The site chosen for the new military headquarters was an area of swamps and garbage dumps at the edge of Washington, D.C., where construction began on September 11, 1941. Just 16 months after the groundbreaking, on January 15, 1943, the building was dedicated. The entire cost of the project, including outside facilities, was \$83 million.

A vast structure, the Pentagon covers 29 acres (11.74 hectares) and comprises three times as much floor space as the Empire State Building in New York City. Any one of its five wedge-shaped sections would hold the entire U.S. Capitol Building. Workplace for some 23,000 civilian and military employees, it has 17.5 miles of corridors, yet it takes only seven minutes to walk between any two points in the building. On September 11, 2001—exactly 60 years to the day after construction began on the building—terrorists flew American Airlines Flight 77 into the side of



Department of Defense photo showing the Nassr Engineering Manufacturing facility in Iraq destroyed in 1998, and rebuilt in 2002. Analysts at the Defense Department determined that the rebuilt facility had the capability to produce precision components for nuclear missiles. AP/WIDE WORLD PHOTOS.

the Pentagon, killing over one hundred personnel inside, as well as the people aboard the plane.

## DOD Resources

Since the time of the terrorist attacks, DOD has been tasked with the protection of national security through a number of operations, most notably Enduring Freedom in Afghanistan during late 2001 and 2002, and Iraqi Freedom in early 2003. Always important, its significance has become vastly greater since September 2001. Americans following the course of the wars overseas have seen their tax dollars put to use through the deployment of highly trained and equipped troops assisted by the most advanced military technology on Earth.

In almost every regard, the resources available to DOD are remarkable. First among those are the human resources, including 1.4 million active-duty military personnel and 654,000 civilian employees as of 2002. In addition, some 1.2 million serve in the National Guard and

Reserve forces. The DOD workforce is also highly trained: whereas 79 percent of working-age Americans have high-school diplomas, 95 percent of DOD employees do, and 5.6 percent of all DOD personnel have master's degrees, as compared to 4.9 percent of the total U.S. work force.

DOD's civilian and active-duty workforce of 2 million makes it among the nation's largest employers, while its budget of \$371 billion in 2002 gives it a bottom line far beyond the scope of corporations in the private sector. For comparison, Wal-Mart, with its vast reach, had annual revenues of \$227 billion, with 1.3 million employees, in 2001.

When it comes to ownership and management of property, no entity in the private sector can compare with DOD, whose comprehensive inventory of facilities and installations in August, 2002, showed that it was landlord to some 600,000 individual structures at more than 6,000 different sites worldwide. These ranged from tiny unoccupied stations housing a single navigational aid to the Army's enormous White Sands Missile Range in New Mexico, which comprises over 3.6 million acres (5,625 sq. mi.; 14,569 sq. km.)—about the size of Connecticut. In all,

DOD controls some 30 million acres (46,875 sq. mi.; 121,406 sq. km.), an area a little larger than Pennsylvania.

**Leadership.** Ultimate leadership of DOD rests with the commander-in-chief, the president of the United States. According to the U.S. Constitution, it is the president, the senior military authority, who is responsible for protection of the nation against all enemies, foreign and domestic. The president exercises that authority through two entities that did not exist at the time the Constitution was written: the secretary of defense and the NSC.

Working with these two, the president determines the priorities of national security, and then takes action to ensure that those needs are met. The authority of these executive entities is checked and balanced by that of Congress, which has the power to approve or reject budgets, and whose various committees oversee funding, military operations, and intelligence. Congress exercises oversight in areas ranging from major troop deployments to pay raises.

**The Secretary.** “National Command Authority” (or “national command authorities”) is a term referring to the president and the secretary of defense together. They constitute both a chain of command and, in certain cases, a single commanding entity, though of course the president always has the power to override the secretary.

Notable secretaries of defense have included George C. Marshall (1950–51) under President Harry S. Truman; Robert S. McNamara (1961–68) under presidents John F. Kennedy and Lyndon B. Johnson; Caspar Weinberger (1981–87) under President Ronald Reagan; and Richard Cheney (1989–93) under President George H. W. Bush. In 2001, Cheney became vice president for President George W. Bush, with Donald Rumsfeld—who had served as secretary of defense for President Gerald R. Ford becoming the first secretary to serve nonconsecutive terms.

The Office of the Secretary of Defense carries out policy by assignments to the military departments, which train and equip the military forces; the Chairman of the Joint Chiefs of Staff (JCS), who plans and coordinates military deployment and operations with other JCS members; and the unified commands, which conduct and carry out military operations.

**The Joint Chiefs of Staff.** The Joint Chiefs of Staff consists of a chairman, vice chairman, and the four heads of the DOD military services (Army, Navy, Air Force, and Marines), each of whom is a four-star general. The chairman sits on the NSC, to which he is principal military advisor. Assisted by the other members of JCS, he plans and coordinates military operations at the National Military Command Center, commonly called “the war room.”

During times of military action, the JCS chairman often serves as a public face for the military, conducting

high-level media briefings either alongside the secretary of defense, or on his own. Thus, during the Persian Gulf War in 1991, Americans became accustomed to seeing General Colin Powell, as they would a later JCS chairman, Richard Myers, during operations Enduring Freedom and Iraqi Freedom. (Powell, by then secretary of state for George W. Bush, remained a visible figure.)

**Unified commands.** Actual fighting during wartime is overseen, not by the services themselves, but by the nine unified military commanders. In peacetime, the secretary of defense, acting through the three service secretaries (of the Army, Navy, and Air Force) exercises authority over the training and equipping of troops. In wartime, he exercises authority through the unified commanders, with the advice of the JCS chairman.

On October 1, 2002, DOD established a new Unified Command Plan to prepare it for the wars of the twenty-first century, including the action in Iraq for which U.S. forces were already preparing. The new plan solidified a trend toward unified command that had been taking place in the military for several decades, as leaders recognized the need for integrated warfighting capabilities.

**Geographic commands.** Of the nine unified commands, five have specific geographic responsibilities. Largest among these is the European Command, whose area of operations extends well beyond Europe, and encompasses 93 nations across 13 million square miles (33,669,850 sq. km.) between the North Cape of Norway and the Cape of Good Hope at the southern tip of Africa, and from the eastern half of the Atlantic Ocean to the Caspian Sea.

Central Command is a name familiar from Operation Iraqi Freedom and other Mideastern deployments, but the word “central” in the title does not mean that it is central command for the entire U.S. military. Rather, it refers to the command’s area of operations, in the center of the Eastern Hemisphere, a region that encompasses the Middle East, northeastern Africa, western Asia, and part of the Indian Ocean.

The Northern Command encompasses the continental United States, Canada, Alaska, Central America, and the Caribbean, while the Southern Command is responsible for South America. Finally, the Pacific Command, which covers the largest geographic area—about 50% of Earth’s surface, most of it ocean—includes east Asia, Oceania, and the Pacific islands, and shares responsibility for Alaska with the Northern Command.

**Non-geographic commands.** DOD describes the Joint Forces Command as the “transformation laboratory” for the U.S. military. It is concerned with finding new solutions for future challenges, for developing joint warfighting capabilities through joint training, and for delivering joint forces and capabilities to warfighting commanders.

Strategic Command controls missile, deterrence, space, and satellite systems. The Special Operations Command comprises a number of special support teams, including the Navy SEALs, Army Special Forces, Delta Force, and so on. Finally, the Transportation Command is responsible for moving personnel and materials around the world.

**Field activities and defense agencies.** In addition to the four services and unified commands, DOD includes seven field activities and 15 defense agencies. The field activities are the American Forces Information Service, Defense Prisoner of War/Missing Personnel Office, Defense Human Resources Activity, DOD Education Activity, TRICARE Management Activity, Office of Economic Adjustment, and Washington Headquarters Services.

Notable defense agencies include the Defense Intelligence Agency, National Imagery and Mapping Agency, and National Security Agency, which, along with the Army, Navy, Air Force, and Marine intelligence components, constitute a majority among the 14 agencies and organizations of the U.S. Intelligence Community. Also significant, from a national security standpoint, are the Defense Security Service, Defense Security Cooperation Agency, Missile Defense Agency, Defense Advanced Research Projects Agency, Defense Information Systems Agency, and Missile Defense Agency.

#### ■ FURTHER READING:

##### BOOKS:

- Cordesman, Anthony M. *Terrorism, Asymmetric Warfare, and Weapons of Mass Destruction: Defending the U.S. Homeland*. Westport, CT: Praeger, 2002.
- Gilmour, Robert S., and Alexis A. Halley. *Who Makes Public Policy?: The Struggle for Control Between Congress and the Executive*. Chatham, NJ: Chatham House Publishers, 1994.
- Ripley, Randall B., and James M. Lindsay. *U.S. Foreign Policy after the Cold War*. Pittsburgh: University of Pittsburgh Press, 1997.
- Trask, Robert R., and Alfred Goldberg. *The Department of Defense, 1947–1997: Organization and Leaders*. Washington, D.C.: Office of the Secretary of Defense, 1997.

##### ELECTRONIC:

U.S. Department of Defense. <<http://www.defenselink.mil/>> (April 28, 2003).

##### SEE ALSO

*Air Force Intelligence, United States*  
*DARPA (Defense Advanced Research Projects Agency)*  
*Defense Information Systems Agency, United States*  
*Defense Nuclear Facilities Safety Board, United States*  
*Defense Security Service, United States*  
*DIA (Defense Intelligence Agency)*  
*Enduring Freedom, Operation*

##### G–2

*INSCOM (United States Army Intelligence and Security Command)*  
*Iraqi Freedom, Operation (2003 War Against Iraq)*  
*Joint Chiefs of Staff, United States*  
*Korean War*  
*Military Police, United States*  
*National Command Authority*  
*National Military Joint Intelligence Center*  
*Navy Criminal Investigative Service (NCIS)*  
*NIMA (National Imagery and Mapping Agency)*  
*NMIC (National Maritime Intelligence Center)*  
*NSA (United States National Security Agency)*  
*NSC (National Security Council)*  
*Persian Gulf War*  
*Special Operations Command, United States*  
*USSTRATCOM (United States Strategic Command)*  
*Vietnam War*

---

## DOE (United States Department of Energy)

---

Though many of its security and intelligence functions have been passed to a subordinate office, the National Nuclear Security Administration (NNSA), the Department of Energy (DOE) is still the principal guarantor of energy security in the United States. It has the task of maintaining the safety and reliability of the U.S. nuclear stockpile, cleaning up the environmental legacy of the Cold War arms race, and advancing science and technology in the service of national interests. In addition to DOE's overall concern for global nuclear security, the DOE Office of Security works to protect employees, DOE contractors, and entrusted assets. Office of Security programs include the Nonproliferation and National Security Institute (NNSI) and the Cyber-Forensic Laboratory. DOE also has an intelligence office that is a component of the U.S. Intelligence Community.

### Background

Most Americans tend to think of DOE in connection with civilian activities—for example, its effect on the price of gasoline at the pump—but in fact it is one of the federal government's most significant security assets. Its roots go back to the Manhattan Project, the successful effort to build an atomic bomb during World War II. Though most of the scientists in the Manhattan Project were civilian, the governing authority was military. Thus, in 1942, the first full year of U.S. participation in the war, the U.S. Army Corps of Engineers established the Manhattan Engineer District to oversee the project.

The war's end saw a heated battle in Congress over the issue of whether to place atomic power under civilian



A trauma intervention volunteer plays the role of a casualty of a simulated gas attack during an inter-agency emergency response drill in Portland, Oregon. AP/WIDE WORLD PHOTOS.

or military control. In 1946, the issue was settled with the passage of the Atomic Energy Act, which created the civilian-run Atomic Energy Commission (AEC). In the early Cold War years, AEC put its greatest emphasis on the production of nuclear weapons, and on the development of nuclear reactors to propel naval vessels. A second Atomic Energy Act, in 1954, opened the field of nuclear power to the private sector, and AEC served as the regulatory agency for the new industry.

As a result of U.S. vulnerabilities in the face of the 1973 Arab oil embargo, Congress in 1974 passed the Energy Reorganization Act, which abolished AEC and replaced it with two other agencies: the Nuclear Regulatory Commission (NRC) and the Energy Research and Development Administration. As the energy crisis of the 1970s wore on, however, it became more and more apparent that the government could most effectively deal with energy issues by unifying energy organization and planning. The result was the Department of Energy Organization Act, signed into law by President James E. Carter on October 1, 1977.

The new department replaced not only the Energy Research and Development Administration, but also the Federal Energy Administration, the Federal Power Commission, and programs or offices of other agencies. (NRC remained independent.) At the outset, DOE took the role of providing a framework for the development of a comprehensive national energy plan. It also undertook long-term, high-risk research and development in areas that included energy technology, energy conservation and regulation, federal marketing of power, energy data collection and analysis, and nuclear weapons.

The period since DOE's inception has seen a shift in focus in view of America's changing needs within the global landscape. Faced with the energy crisis of the late 1970s, DOE directed its efforts toward development and regulation of energy resources. The arms buildup that took place under the administration of President Ronald Reagan in the 1980s saw DOE turn its attention to nuclear weapons research, development, and production. With the end of the Cold War, DOE entered a new phase, in which its emphasis was on nonproliferation, nuclear stewardship, retooling of nuclear weapons for peaceful uses, and environmental cleanup.

## The DOE Today

Energy efficiency and conservation have remained focal points of DOE efforts, particularly in view of increasing tensions with and in the Middle East—where most of the world's oil is produced. In his 2003 State of the Union address, President George W. Bush, pledged \$1.2 billion toward the development of hydrogen-powered fuel cells. Not only would the development of hydrogen power, long an area of research within DOE, free the United States from dependence on Middle Eastern oil, but it would greatly reduce the environmental impact of human activities, and provide an energy resource of almost limitless renewability.

Today, DOE accomplishes its mission along four principal program lines: national defense, energy, the environment, and science. DOE national defense programs, which DOE has continued to list as a top priority, have a

fourfold purpose: to protect U.S. nuclear weapons, to promote nuclear safety internationally, to advance the cause of non-proliferation, and to continue providing safe and effective nuclear power for the operation of U.S. Navy vessels.

In the area of energy, DOE priorities include increasing domestic production, revolutionizing Americans' approach to conservation and efficiency, and promoting the development of renewable and alternative sources—including hydrogen. The environmental program overlaps somewhat with the national defense goal of cleanup of environmental and safety hazards left over from the Cold War. DOE is also committed to the safe and permanent disposal of radioactive waste. There is also overlap between the energy priority and a fourth program area, that of science, in which DOE's greatest interest is revolutionizing the search for, production, and delivery of energy.

Some aspects of DOE's responsibilities for national and global security are the work of NNSA, created by Congress in 1999 as a response to apparent security violations that occurred during the presidency of William J. Clinton. Though NNSA is an agency of DOE, its administrator, an undersecretary within the department, has direct responsibility over most of its functions.

Responsibilities of DOE and NNSA overlap in some areas. For example, both DOE and NNSA are concerned with nonproliferation programs involving Russian and other former Soviet republics. The purposes of these programs include the securing of nuclear weapons, elimination of excess materials, prevention of the outflow of nuclear expertise to other countries, and downsizing of the overall nuclear weapons complex in the former Soviet Union.

A particular area of emphasis in the DOE nonproliferation and verification program is the conversion of highly enriched uranium (HEU) to peacetime uses. In 1994, DOE agreed to purchase 500 metric tons of Russian HEU over the next 20 years, at a cost of \$12 billion. The materials would then be converted to low enriched uranium and applied to commercial uses.

## Emergency Operations

The Emergency Operations (EO) office of DOE is a joint mission of DOE and NNSA, created to administer and direct the emergency response capabilities of both. Focused on nuclear and radiological emergencies, EO is the principal DOE point of contact for emergency management activities.

EO develops policy for the emergency management of sites, facilities, and operations; manages the response to nuclear and radiological emergencies worldwide on behalf of the U.S. government; coordinates inter- and intradepartmental emergency management activities; evaluates and works to improve emergency response capabilities; and seeks to integrate programs, systems,

assets, capabilities, training, and responses to improve emergency capabilities.

**Offices of Emergency Management and Response.** EO consists of two offices, the Office of Emergency Management (OEM) and the Office of Emergency Response (OER). OEM is charged with developing and implementing DOE's emergency management system for DOE and NNSA facilities, sites, and activities. It is responsible for operations and training, direction of emergency response exercises, development of emergency management policies, and support of DOE and NNSA site emergency planning and response.

OER supports both crisis response and emergency management through various departmental radiological emergency response assets or capabilities. It is responsible for the overall program management and organizational structure of EO in both emergency and non-emergency situations. OER also supports federal counterterrorism and consequence management efforts that have a nuclear or radiological dimension. In addition, EO as a whole represents DOE as needed in multiagency responses to nuclear or radiological threats affecting public safety and health.

**Office of Security.** Following the September 11, 2001, terrorist attacks, numerous components of the federal security and intelligence apparatus came under scrutiny, and among these was the DOE Office of Security. In 2002, Representative Ed Markey (D-MA) released figures showing that the number of DOE security forces had dropped from 7,091 in 1992 to just 4,262 in 2001, a reduction of 40 percent. Political and intelligence analysts argued that these reductions were typical of the post-Cold War, Clinton-era reduction in security and intelligence resources, and after September 2001, DOE Office of Security director Joseph C. Mahaley worked to rebuild those resources.

In his role as chief functionary responsible for the development of policy regarding the protection of national security assets under DOE control, Mahaley gave a statement to the U.S. House of Representatives Committee on the Budget on December 5, 2001. In his statement, Mahaley explained that, in accordance with the DOE Security Condition (SECON) system, the office had declared a level 2 emergency (SECON 2) on the day of the terrorist attacks, but had since dropped to—and stayed at—SECON 3, the highest alert level that could be maintained indefinitely.

**Missions and priorities.** The highest DOE security priority, Mahaley explained, is the protection of special nuclear material, or SNM, including everything from raw nuclear materials to complete nuclear weapons. DOE's nuclear safeguards and security program are directed toward preparing for a worst-case scenario involving the theft of these materials.

In addition to its mission of protecting materials and technology—including non-nuclear assets of DOE—the Office of Security also participates in the Technical Support Working Group, an interagency counterterrorism team headed by the State Department. The Office of Security had, at the time of Mahaley's statement, 550 trained counterterrorism personnel in its special response teams at 11 locations, along with 3,500 other armed officers.

**Programs.** Office of Security programs include NNSI, a training provider not only for DOE, but for students from more than 100 government departments and agencies. Founded in 1984 and formerly known as the Central Training Academy, NNSI is located at Kirtland Air Force Base in Albuquerque, New Mexico. Among its schools are the Professional Development Program, the Defense Nuclear Nonproliferation and International Cooperation Academy, the Foreign Interaction Training Academy, the Emergency Operations Training Academy, the Safeguards and Security Central Training Academy, and the Counterintelligence Training Academy.

The last of these, known as CITA, was established in May 2000, and offers instruction to contractor employees as well as federal workers. In addition to full courses, it offers seminars on subjects such as "Counterintelligence for Managers," "Economic Espionage: Protecting Intellectual Property," and "The Technical Collection Threat to Travelers."

The other major Office of Security program is the Cyber-Forensic Laboratory. Cyber-forensics is the application of science and technology to the discovery, analysis, and reconstruction of data extracted from any element of computers, computer peripherals, or computer systems. The laboratory assists DOE with the collection and study of electronic data relating to DOE security, or that of other government agencies and departments.

**Office of Intelligence.** DOE's Office of Intelligence (IN) is a member of the U.S. Intelligence Community (IC), producing intelligence for use both within DOE, and across the IC as a whole. Within the IC, the Office of Intelligence is the leading technical intelligence resource in four areas: nuclear weapons and nonproliferation; nuclear energy, safety, and waste; science and technology; and energy security.

The mission of IN within the IC is three-fold: to provide DOE and other agencies and departments, particularly IC members, with timely, accurate, and effective analyses of foreign intelligence; to make DOE's expertise available to the intelligence, law enforcement, and special operations communities; and to provide timely, specialized technological applications and operational support to those communities.

Presidential Decision Directive (PDD) 61, issued by President Clinton in February 1998, reorganized the intelligence structure at DOE. Counterintelligence and foreign intelligence functions were separated, and both offices were made directly answerable to the secretary of energy.

The new counterintelligence director would be a senior Federal Bureau of Investigation (FBI) executive, and would have direct access to the directors of Central Intelligence and the FBI as well as the secretary of energy. In conjunction with the Office of Security, the director would work to implement specific security measures designed to reduce the threat to classified and sensitive information at DOE.

DOE operates a number of national laboratories that bring together scientists from a variety of disciplines to work on military and non-military related projects. National laboratory scientists have developed a number of technologies related to national security interests.

## ■ FURTHER READING:

### BOOKS:

*Closing the Circle on the Splitting of the Atom: The Environmental Legacy of Nuclear Weapons Production in the United States and What the Department of Energy Is Doing About It.* Washington, D.C.: U.S. Government Printing Office, 1995.

*Department of Energy Non-Proliferation Programs with Russia: Hearing Before the Committee on Foreign Relations, United States Senate, One Hundred Seventh Congress, First Session, March 28, 2001.* Washington, D.C.: U.S. Government Printing Office, 2001.

Rudman, Warren B. *Science at Its Best, Security at Its Worst: A Report on Security Problems at the U.S. Department of Energy.* Washington, D.C.: President's Foreign Intelligence Advisory Board, 1999.

### PERIODICALS:

Carr, Rebecca. "Security at Nuke Labs Lax—DOE 'Indifferent' Despite Sept. 11." *Atlanta Journal-Constitution.* (August 20, 2002): A11.

### ELECTRONIC:

Department of Energy. <<http://www.energy.gov>> (March 7, 2003).

Department of Energy Office of Security. <<http://www.so.doe.gov>> (March 7, 2003).

### SEE ALSO

*Cold War (1945–1950), The Start of the Atomic Age Energy Technologies Intelligence Community NNSA (United States National Nuclear Security Administration)*

---

## Domestic Emergency Support Team, United States

---

Up to the time of its transfer to the newly created Department of Homeland Security (DHS), the Domestic Emergency Support Team (DEST) was the smallest—or, at



least, the most obscure—of the Justice Department offices dedicated to national security and intelligence. It was created under Presidential Decision Directive 39 (PDD 39), “U.S. Policy on Counterterrorism,” signed by President William J. Clinton on June 21, 1995. That document called for a “rapidly deployable interagency emergency support team” to assist the State Department in situations of emergency involving U.S. citizens on foreign soil, as well as for a DEST to operate in domestic incidents under the direction of the Federal Bureau of Investigation (FBI).

According to PDD 39, “The DEST shall consist only of those agencies needed to respond to the specific requirements of the incident,” indicating that DEST is not so much an office unto itself as it is a coordinating agency. Its function is not only to respond to terrorist incidents; in July 2002, for instance, DEST went on call in response to flooding in Texas. However, President George W. Bush made clear its place in the post-September 11, 2001, security environment by including DEST in the Homeland Security Act, which he sent to Capitol Hill on June 18, 2002. Title V, “Emergency Preparedness and Response,” established the position of under secretary for Emergency Preparedness and Response, whose duties would include oversight of DEST. DEST was one of several agencies transferred from Justice to DHS when that department began functioning in March 2003.

#### ■ FURTHER READING:

##### PERIODICALS:

Reiss, Tom. “Now Will We Heed the Biological Threat?” *New York Times*. (February 21, 1998): 11.

##### SEE ALSO

*FBI (United States Federal Bureau of Investigation)*  
*Homeland Security, United States Department*

## Domestic Intelligence

Domestic intelligence is a term for efforts by a government to obtain information about activities that pose an actual or putative threat to internal security. In authoritarian or totalitarian regimes, domestic intelligence-gathering by the government is a regular part of daily life, but in a liberal democratic system such as those of North America or Western European countries, it is more problematic. United States domestic intelligence programs of the post World War II era raised Americans’ ire after they came to light, but in the wake of the September, 2001, terrorist attacks, many Americans and Europeans put aside fears of



A pedestrian passes under the arm of a traffic surveillance system in the Chelsea neighborhood of New York City. AP/WIDE WORLD PHOTOS.

government surveillance in favor of a new demand for heightened security.

**World War II to Watergate.** Whereas most Americans of the postwar era knew that the intelligence services of the Soviet Union and other totalitarian states kept a close watch on their citizens, most had no idea of the extent to which their own government was watching certain elements. During the 1970s and later, information about massive domestic intelligence programs came to light. Among these was Shamrock, which involved the interception of telegrams and other forms of communication between 1945 and 1975. In another domestic intelligence/surveillance program, Chaos, the Federal Bureau of Investigation (FBI) monitored Vietnam War protesters between 1967 and 1972, looking for ties to the Soviets.

Revelation of these and other activities came to light in the wake of the Watergate scandal, which influenced an attitude among some citizens of suspicion toward the government. Questionable as they may have been in some regards, Shamrock and Chaos subjected only a fraction of the population to government scrutiny, but in the atmosphere of reaction that pervaded the mid- to late



1970s, many Americans began to assume that there was no limit to the government's desire for information on its citizens' private lives. These fears both led to, and were fueled by, investigations in Congress, most notably that of the Church Committee in the Senate.

**The twenty first century.** Since that time, government agencies have been placed under much tighter restrictions with regard to domestic intelligence and surveillance. The September, 2001, attacks, however, influenced a shift in a different direction. Congress, once suspicious of domestic intelligence-gathering, called for a new effort to root out potential terrorists on U.S. soil. The same was true in Europe, where countries such as Belgium—which had always restricted domestic intelligence efforts—gave their internal security services much freer rein.

During 2002, the U.S. executive and legislative branches debated the question of which agency should handle a new domestic intelligence effort: the FBI (formerly in charge of counterterrorism) or the Central Intelligence Agency (CIA). In February 2003, President George W. Bush placed the CIA in charge of a new domestic counterterrorism intelligence agency, to be formed later that year. The FBI would work with the CIA in the new unit.

#### ■ FURTHER READING:

##### BOOKS:

- Alden, Edward, and James Harding. "CIA Wins Battle to Defend U.S. Against Terror." *Financial Times* (February 15, 2003): 1.
- Crawford, David. "Europe Eases Limits on Police, Intelligence Services—Fear of Islamist Terrorism Erodes Traditional Divide Between the Two Branches." *Wall Street Journal* (December 17, 2002): A15.
- EGgen, Dan. "Bush Aims to Blend Counterterrorism Efforts." *Washington Post* (February 15, 2003): A16.
- Johnston, David. "FBI Director Rejects Agency for Intelligence in United States." *New York Times* (December 20, 2002): A22.
- Lichtblau, Eric. "FBI and CIA to Move Their Counterterror Units to a Single New Location." *New York Times* (February 15, 2003): A14.
- Polmar, Norman, and Thomas B. Allen. *Spy Book: The Encyclopedia of Espionage*. New York: Random House, 1998.
- Priest, Dana, and Juliet Eilperin. "Panel Finds No 'Smoking Gun' in Probe of 9/11 Intelligence Failures." *Washington Post* (July 11, 2002): A1.

##### SEE ALSO

*Church Committee*  
*CIA, Legal Restriction*  
*Domestic Intelligence*  
*FBI (United States Federal Bureau of Investigation)*  
*Intelligence and democracy: Issues and Conflicts*  
*Intelligence, United States Congressional oversight*  
*Nixon Administration (1969–1974), United States National Security Policy*  
*Operation Shamrock*

*Privacy: Legal and Ethical Issues*  
*September 11 Terrorist Attacks on the United States*  
*United States, Counter-terrorism Policy*  
*Watergate*

## Domestic Preparedness Office (NDPO), United States National

Formed in October 1998, the United States National Domestic Preparedness Office (NDPO) is the coordination center for all federal efforts in response to weapons of mass destruction (WMD). It works with a variety of federal agencies, and assists state and local emergency responders in preparing for the response to a WMD event. The Federal Bureau of Investigation (FBI) originally formed NDPO, which became part of the Department of Homeland Security (DHS) in March 2003.

An August, 1998, stakeholders conference involving leading members of the federal emergency response community resulted in a recommendation that a single office coordinate all federal WMD preparedness assistance programs. The result was the creation of NDPO by Attorney General Janet Reno, who placed the FBI in charge of the new office, initially known as the Office for State and Local Domestic Preparedness.

NDPO works in partnership, not only with the FBI, but also with the departments of Energy, Health and Human Services, and Justice; the Federal Emergency Management and Environmental Protection agencies; the Office for State and Local Domestic Preparedness Support; and the National Guard Bureau. Its mission is to coordinate and facilitate all federal WMD efforts to assist state and local responders in their response to a WMD event. This requires assistance in planning, training, equipment, exercise, and health and medical issues.

#### ■ FURTHER READING:

##### PERIODICALS:

- "Training Centers Offer Assistance." *Crime Control Digest* 36, no. 18 (May 3, 2002): 11.
- Vise, David A. "Senate Panel Blasts FBI's Deployment." *Washington Post*. (July 21, 2000): A29.

##### ELECTRONIC:

- National Domestic Preparedness Office. Federation of American Scientists. <<http://www.fas.org/irp/agency/doj/fbi/ndpo/>> (March 28, 2003).
- Office of Domestic Preparedness. U.S. Department of Justice. <<http://www.ojp.usdoj.gov/odp/>> (March 28, 2003).

## SEE ALSO

*FBI (United States Federal Bureau of Investigation)  
Homeland Security, United States Department  
Weapons of Mass Destruction*

## Doo Transmitter

A Doo radio transmitter, officially known as a T-1151 radio transmitter, is a radio transmission device camouflaged as a pile of animal droppings or, in its most common form, a large single fecal dropping from an animal indigenous to the area of intended use. Regardless, the external form of the device was designed to discourage close examination and thus, detection or disruption.

Initially developed by United States military intelligence about 1970, the Doo transmitter was a homing device camouflaged as dog or monkey feces for use in Vietnam. At just over four inches long and three-quarters of an inch in height, this inconspicuous spy tool was small enough to be carried easily. It could send or receive radio messages, usually by Morse code. The effectively camouflaged beacon was positioned throughout the jungles of Vietnam, where it transmitted a radio signal that helped aircraft pinpoint key enemy ground sites for strikes or reconnaissance. The device often had a peat moss crusted shell.

Because the Doo transmitter was often left undisturbed, operational life was often a function of the battery life of its nickel-cadmium battery array. This advantage was often essential when the transmitter was utilized as a homing device. Because the device gave the appearance of fecal matter, it was often left undisturbed and thus a retained high efficiency as a homing beacon even when planted days or weeks before a mission.

Another operational advantage of the Doo transmitter was its capacity to remain concealed long after its operational usefulness ended. Accordingly, in addition to detection avoidance while operational, the long-term detection avoidance qualities of the transmitter did not allow the enemy the intelligence advantages of knowing that a particular site was at one time used as a transmission or rendezvous point.

The Doo transmitter design reflects an open concealment design concept used by intelligence agencies. Such open concealment devices remain easily visible, only the operational nature of the device is concealed.

## SEE ALSO

*Shoe Transmitter  
Short-Wave Transmitters  
Vietnam War*

## Doppler Radar.

SEE *Stealth Technology.*

## Dosimetry

■ LARRY GILMAN

Dosimetry measures the amount of radiation energy absorbed over a given period of time by an object (e.g., human body) or by part of that object (e.g., an organ or tumor). Here, radiation refers not only to ionizing radiation of the sort emitted by radioactive materials—fast particles and gamma rays—but to light, radio waves, or ultrasound. Dosimetry is essential wherever radiation is utilized to treat cancer; the treatment must deliver a sufficient dose to target tissues without delivering too large a dose to other parts of the body. Dosimetry is also needed, wherever radioactive materials are handled in significant quantities, to track the cumulative exposure of individuals and to monitor for accidental releases of radioactive material.

A device that measures cumulative radiation exposure is a *dosimeter*. A Geiger counter is a radiation detector, but not a dosimeter, because it gives only a moment-to-moment reading of radiation intensity; a strip of photographic film, however, whose degree of exposure indicates how much radiation it has absorbed (up to its saturation limit), can act as a dosimeter. Filmstrip dosimeters are, in fact, still used to measure exposure to ionizing radiation. By grading the sensitivity of a specially formulated film strip from one end to the other, it can be made to indicate net, cumulative radiation exposure as a bar of darkening that grows from the most sensitive end of the film to the least sensitive end. Such “badge dosimeters” are common in the nuclear weapons and nuclear-power industries. However, they have the disadvantage that they must be developed to be read, and so do not give the bearer immediate knowledge of their exposure level.

Another type of dosimeter is the pen ionization dosimeter. These devices contain a long, narrow chamber filled with a few cubic centimeters of nonconducting gas. A metallic contact touches the interior of the chamber at each end. When the dosimeter is to be used, an initial electric charge is placed on the gas tube; that is, an imbalance of electrons is created between the two ends. Since the gas in the tube is normally nonconducting, electrons cannot travel through it to even out the charge imbalance. However, ionizing radiation passing through the gas forcibly frees electrons from atoms in the gas (i.e., partly ionizes the gas), and these negatively charged electrons are free to flow toward the end of the tube having a positive charge. The more ionizing radiation the pen dosimeter is exposed to, therefore, the more of its initial

charge is enabled to leak through the gas tube; the amount of charge lost is a measure of the amount of radiation that has passed through the tube. A pen dosimeter can be read by its bearer at any time, and so gives a current reading of exposure; however, pen dosimeters readings can be affected by mechanical shock or vibration.

A more modern dosimeter design is the thermoluminescent dosimeter (TLD). A TLD contains a tiny crystal of lithium fluoride (sometimes mounted in a finger-ring) that undergoes cumulative structural changes as it is exposed to ionizing radiation. When heated, the crystal glows, giving off an amount of light that is proportional to its radiation exposure. This light is observed by an electronic sensor in a readout unit and recorded digitally. This data can be stored in a central database, a convenient feature if an organization wishes to systematically monitor radiation exposure of a large body of personnel. Databasing of TLD data has been used, for example, by Canada to monitor the exposure of its troops to radiation from depleted-uranium munitions used by NATO in Bosnia. TLDs, unlike film badges, can be re-used; however, they must be inserted in a reader that heats the crystal and records the light emitted, a process that may take 20 to 30 seconds and erases the data in the crystal.

An even more recent entry in the dosimeter field is the optically stimulated luminescence dosimeter (OSLD). In this design, a thin film of crystalline aluminum oxide undergoes cumulative structural changes as it is exposed to ionizing radiation; when an exposure reading is desired, the crystal is exposed to green laser light. The amount of blue light emitted by the film in response is proportional to its radiation exposure. Unlike a TLD, an OSLD can supply an instant readout that can be repeated if necessary.

Solid-state devices that measure radiation by detecting ionization leakage current through a transistor device also exist. Radiation detectors and dosimeters based on such solid-state technology have been available since the 1980s, but have not edged out other dosimeter technologies in terms of cheapness, sensitivity, and accuracy.

Dosimetry for laser light, radio waves, and ultrasound, which is often required in medical contexts, is more difficult than dosimetry of ionizing radiation. One method of measuring dose delivered to a volume of tissue is to measure the temperature increase of the tissue; the more increase, the more radio or sound energy has been absorbed. However, these techniques do not work for tissue embedded in living organisms (where temperature measurement is difficult and where heat is rapidly conducted away) or for whole-body exposure, as biologically tolerable doses of laser, radio, and sound energy produce undetectably slight changes in body temperature. Absorption by the body of radio waves is particularly different from absorption of ionizing radiation; the body acts as a complex antenna whose performance is strongly affected by its posture and orientation and by nearby objects. Dosimetry for radio and ultrasound therefore relies heavily on computational models rather than on direct measurements.

## ■ FURTHER READING :

### ELECTRONIC:

"Measuring Occupational Exposures." Health Physics Society. <<http://hps.org/publicinformation/ate/faqs/lowmeasure.html>> (April 17, 2003).

"Using and Wearing Radiation Dosimeters." Princeton University: Environmental Health and Safety. <<http://www.princeton.edu/~ehs/UsingandWearingDosimetry.html>> (April 17, 2003).

### SEE ALSO

*Radiation, Biological Damage*

*Radioactive Waste Storage*

*Radiological Emergency Response Plan, United States Federal*

---

## Double Agents

---

A double agent is person who conducts espionage for two, usually antagonistic, countries. Double agents allow intelligence services to gather information by infiltrating enemy organizations under cover. An organization usually recruits double agents from the ranks of a rival intelligence service, and then "turns" them, using them as spies for their own purposes.

The use of double agents in intelligence tradecraft and strategy is one of the oldest practices in the art of espionage. Spies and double agents appear in literature and written histories from the ancient civilizations of Egypt, China, India, Greece, and Rome. The rise of great civilizations and militaries prompted the need for intelligence gathering through infiltration of enemy organizations.

In the modern era, double agents gained notoriety in a variety of espionage scandals. While some double agents worked in accordance with their ideals, others were paid handsomely with money or political favor for betraying secrets. During the Cold War between the United States and the Soviet Union, exposure of double agents became a key part of counterintelligence operations. Double agents compromised intelligence, military, industrial, and government strongholds in both nations, sometimes with devastating consequences. Since the fall of the Soviet Union, and the dissolution of its KGB intelligence agency, access to formerly secret archives and testimony of former agents has exposed several double agents, and the extent of their decades-long espionage operations. In the United States, double agents working for the Soviet Union (and later for Russia), such as Aldrich Ames and Robert Hanssen were discovered, brought to trial, and sentenced to life in prison.

During the Cold War, and the decade after its end, double agents were popularly associated with intrigue,



Harold "Kim" Philby (standing) is shown during a 1968 news conference after being cleared of allegations that he was the "third man" who tipped off diplomats Guy Burgess and Donald Maclean. In fact, Philby led a spy ring of former Cambridge University students, including Burgess and Maclean, for the Soviet Union. ©BETTMANN/CORBIS.

and trials of double agents gained extensive media attention. However, within the intelligence community, the use of trained double agents waned. Intelligence services replaced human intelligence operations with an increasing reliance on satellite and electronic surveillance technology. Technological surveillance permits intelligence organizations to conduct operations without assuming the high risks associated with using human intelligence or double agents exclusively.

#### ■ FURTHER READING:

##### ELECTRONIC:

United States Federal Bureau of Investigation. <<http://www.fbi.gov/libref/historic/famcases/hanssen/hanssen.htm#anchor26782>> (April 2003).

The Center for Counterintelligence and Security Studies. <[http://www.cicentre.com/Documents/DOC\\_Hanssen\\_1.htm](http://www.cicentre.com/Documents/DOC_Hanssen_1.htm)> (April 2003).

##### SEE ALSO

*Ames (Aldrich H.) Espionage Case*

*CIA (United States Central Intelligence Agency)*

*Dead Drop Spike*

*Dead-Letter Box*

*FBI (United States Federal Bureau of Investigation)*

*Hanssen (Robert) Espionage Case*

*KGB (Komitet Gosudarstvennoi Bezopasnosti, USSR Committee of State Security)*

## Drop

"Drop" is intelligence parlance for the location at which an agent passes information to another, or the act of passing that information—as in "making a drop." In a live drop, the two individuals actually meet. Given the dangers of this, it is more common to employ a "dead drop." The latter term refers to a prearranged spot at which one party passes information to another without actually meeting. Often a dead drop—a term that again refers both to the place and the act—also involves the transfer of money, as when a double agent leaves information for a handler, and the handler returns the favor with cash payment.

It so happens that the most commonly cited examples of drops and dead drops involved agents working for the Soviet bloc during the Cold War. This is probably the case because, for obvious reasons, Western intelligence agencies are not as likely to reveal the methods employed by their own agents.

One oft-cited example is that of John Walker, who passed \$1 million of United States Navy secrets to the Soviets before the Federal Bureau of Investigation (FBI) finally caught up with him in 1985. In making his drops, Walker used a garbage bag containing bits of recognizable trash—but nothing that would smell strongly and attract animals—along with documents and other important materials. His KGB handler would in turn leave another bag containing money.

In the same year the FBI caught Walker, the Soviets recruited the FBI's own Robert Hanssen, who accumulated \$1.4 million for betraying his country before the authorities caught him in February 2001. At the time of his arrest, Hanssen was making a dead drop under a footbridge at Foxstone Park in Vienna, Virginia.

#### ■ FURTHER READING:

##### BOOKS:

Nash, Jay Robert. *Spies: A Narrative Encyclopedia of Dirty Deeds and Double Dealing from Biblical Times to Today*. New York: M. Evans, 1997.

Polmar, Norman, and Thomas B. Allen. *Spy Book: The Encyclopedia of Espionage*. New York: Random House, 1998.

## ELECTRONIC:

"Traitorous Actions": FBI Agent Charged With Spying for Moscow. <<http://abcnews.go.com/sections/us/DailyNews/FBIarrest010220.html>> (February 1, 2003).

## SEE ALSO

*Cambridge University Spy Ring*  
*Dead Drop Spike*  
*Hanssen (Robert) Espionage Case*  
*Walker Family Spy Ring*

## Drug Control Policy, United States Office of National

■ JUDSON KNIGHT

The White House Office of National Drug Control Policy, or ONDCP, is an independent office of the executive branch of the United States government, and reports directly to the president. Established by the Anti-Drug Abuse Act of 1988, ONDCP is the principal architect of national drug control strategy. It directs anti-drug efforts, and establishes a gameplan for achieving goals, along with a budget and guidelines for cooperation between federal, state, local, and private entities.

**Enabling legislation.** The Anti-Drug Abuse Act of 1988, which set a policy goal of creating a "drug-free America," included as one of its key provisions the establishment of ONDCP. It is charged with setting priorities for anti-drug policy, implementing a national strategy for fighting drugs, and certifying federal drug-control budgets. The drug-fighting strategy, as specified by the statute, must be comprehensive and founded in research; must contain measurable objectives and long-range goals; and must seek reductions in drug abuse, trafficking, and the consequences thereof. Specific aims include the discouragement of drug abuse among young people, a reduction in the number of drug users, and decrease in the availability of drugs.

A series of executive orders in 1993 (E.O. 12880) and 1996 (12992 and 13023) collectively placed ONDCP in the lead role for drug policymaking entities within the executive branch of the federal government. In 1994, the Violent Crime Control and Law Enforcement Act added to ONDCP's responsibilities the assessment of budgets and resources related to the overall national drug control strategy.

The 1997 Drug-Free Communities Act empowered ONDCP to undertake a national initiative whereby federal grants would go to community coalitions with a demonstrated record of reducing substance abuse among local

populations, encouraging cooperation between the private and public sectors, and involving citizens in anti-drug efforts. In 1998, the ONDCP Reauthorization Act expanded ONDCP's role and established additional requirements for the office, including the development of a long-term national strategy for combating illegal drug use and distribution.

**Anti-drug advertising.** Also in 1998, the Media Campaign Act charged ONDCP with leading a national media campaign directed toward young people. This placed the office in collaboration with the Partnership for a Drug-Free America (PDFA), a private organization to which advertisers donate resources as a means of discouraging drug use among America's youth. ONDCP in 1998 initiated the National Youth Anti-Drug Media Campaign, which mobilized both the private and public sectors to fight drug use among young people.

Four years later, a private survey commissioned by ONDCP found that advertising had done little to discourage drug use among adolescents. However, PDFA chairman Jim Burke asserted in a *Washington Post* editorial that this assessment was too pessimistic: not only had drug use among teens not increased, but the advertising had helped to raise awareness among parents.

An ONDCP-sponsored campaign that established a connection between drugs and terrorism drew fire from some critics when it debuted at the 2002 Superbowl. While the connection between the heroin trade and terrorist groups such as al-Qaeda has been established, critics maintained the link between terrorism and drugs is less obvious for marijuana, some of which is grown in the United States. Furthermore, in the view of some detractors, the introduction of the terrorism theme complicated what should have been a simple message discouraging drug use for health and social reasons. Nevertheless, the campaign sparked debate and awareness for personal responsibility issues regarding the global implications for illegal drug purchase and use.

### ■ FURTHER READING:

#### BOOKS:

Ojeda, Auriana. *Drug Trafficking*. San Diego, CA: Greenhaven Press, 2002.

Thompson, Stephen P. *The War on Drugs: Opposing Viewpoints*. San Diego, CA: Greenhaven Press, 1998.

#### PERIODICALS:

Burke, Jim. "Kids, Drugs, and Bureaucrats." *Washington Post*. (May 21, 2002): A17.

Grimm, Matthew. "A Dubious Pitch." *American Demographics* 24, no. 5 (May 2002): 44–46.

"ONDCP Says Anti-Drug Ads Are Ineffective." *Crime Control Digest* 36, no. 20 (May 17, 2002): 4.

**ELECTRONIC:**

White House Office of National Drug Control Policy. <<http://www.whitehousedrugpolicy.gov/>> (February 22, 2003).

**SEE ALSO**

*DEA (Drug Enforcement Administration)*  
*NDIC (Department of Justice National Drug Intelligence Center)*

---

## Drug Intelligence Estimates

---

■ CARYN E. NEUMANN

The National Drug Intelligence Estimate (NDIE), an annual publication of Royal Canadian Mounted Police (RCMP) from 1985 until 1994, identified trends in drug abuse and centers of drug trafficking. NDIE grew out of the realization that illegal drug production, use, and transit affects all countries and that effective international cooperation required an exchange of information. NDIE received wide distribution within Canada and among those countries officially recognized by Canada.

As the Cold War wound down in the 1980s, new elements in the international drug trade emerged at the same time that significant intelligence resources in Western countries became available to combat drug trafficking. The rise in both the supply of drugs and the number of traffickers combined with the reduction of international hostilities to open the possibility of increased international anti-drug trade cooperation. Accordingly, in 1984, the United Nations General Assembly pushed member countries to strengthen and enhance international cooperation in criminal matters relating to the illegal traffic in narcotic drugs. Canada responded to this call by creating NDIE.

The RCMP received the assignment to assemble and distribute NDIE because it is the Canadian agency that is charged with enforcing the nation's drug control laws by apprehending those individuals and organizations involved in illicit drug activities. The Strategic Analysis Branch of the RCMP's Drug Enforcement Directorate produced NDIE as well as regular digests of drug trends and a series of special reports on such matters as money laundering, outlaw motorcycle gangs and aerial cocaine smuggling into Canada. The publications worked together to provide law enforcement personnel with an accurate picture of Canada's relationship to the international drug trade. The RCMP distributed NDIE to all federal departments concerned with drug law enforcement. Provincial and local drug enforcement units also received copies of the estimate, as did RCMP liaison officers stationed at Canadian

embassies who shared the information with their host countries.

NDIE revealed a number of trends in drug smuggling. It reported that while some drugs are produced and consumed domestically, much of the drug trade flowed from developing to developed nations. It predicted that drug incidents involving former citizens of the Soviet Union and its Eastern European allies would increase because the collapse of these countries had left the residents in desperate economic straits and vulnerable to exploitation by both domestic and foreign drug trafficking groups. NDIE identified three threats relating to these ex-communist countries: 1) the shipment of Colombian cocaine to Eastern Europe and then to the West; 2) the increased cultivation of opium in the former Soviet republics of Central Asia and its manufacture into heroin and subsequent shipment through Baltic ports; and 3) the production of amphetamines in places like Poland and their distribution to the West.

Heroin, the illegal narcotic of choice in most of the world and a drug increasing in popularity in the 1990s, received particular attention. NDIE indicated that heroin from Southwestern Asia supplied between twenty and forty percent of the Canadian market in the mid and late 1980s, a rate that rose to 65% in the early 1990s. In 1993, the last year of the estimate, Canadian police seized 154 kilograms of heroin, a 30% increase over seizures in 1992. Record seizures were made in Vancouver and Toronto, which joined Montreal as major centers of heroin trafficking and abuse. The primary heroin entry points into Canada were identified as Halifax, Montreal, Toronto, Winnipeg, and Vancouver.

In the wake of the Cold War, many intelligence agencies redefined their role to include the international drug trade as a major concern along with terrorism and nuclear proliferation. NDIE helped to change the view of the drug trade by identifying it as a global concern that could only be changed by international anti-crime cooperation.

**■ FURTHER READING:****ELECTRONIC:**

Lee, James. "Drugs and Drug Trafficking." November 1996. <<http://www.parl.gc.ca/information/library/PRBpubs/bp435-e.htm>> (April 7, 2003).

Stamler, R.T., R.C. Fahlman and G.W. Clement. "Co-operation Between Canada and Other Countries and Territories to Promote Countermeasures against Illicit Drug Trafficking." United Nations Office on Drugs and Crime Bulletin on Narcotics. January 1, 1987. <[http://www.undcp.org/odccp/bulletin/bulletin\\_1987-01-01\\_1\\_page009.html](http://www.undcp.org/odccp/bulletin/bulletin_1987-01-01_1_page009.html)> <[http://damtp.cam.ac.uk/user/gr/public/gal\\_milky.htm](http://damtp.cam.ac.uk/user/gr/public/gal_milky.htm)> (April 7, 2003).

**SEE ALSO**

*Canada, Intelligence and Security*  
*Cold War (1972–1989): The Collapse of the Soviet Union*

## Dual Use Technology

■ JUDSON KNIGHT

The phrase “dual use technology” refers to tools or techniques, developed originally for military or related purposes, which are commercially viable enough to support adaptation and production for industrial or consumer uses. Examples of dual use technology, for which the United States Department of Defense (DOD) has an entire dedicated program, include capabilities of the U.S. Navy that could be adapted for aviation safety, detecting hazards on the ocean floor, and finding abnormalities in an x ray. As promising as dual-use applications are, their potential for theft or appropriation by hostile powers has led to calls for greater controls over their export.

### Armies and Technology in History

A line of argument commonly heard among foes of the military, or of a strong military defense, is that money spent on defense projects could be better used toward improving society by providing jobs, raising the standard of living, and solving daily problems. In fact, four millennia of human experience support the claim that spending on the development of new military technology ultimately serves to benefit society.

Probably the first example of this principle in action is the Egyptian adoption of the chariot, which greatly advanced the technology of transportation in the second millennium B.C. Had it not been for the invasion by the Hyksos in c. 1670 B.C., who dealt the Egyptians a brutal blow with their chariot-equipped cavalry, Egyptian civilization might never have adopted the chariot.

In c. 800 B.C., the Assyrians introduced foundational concepts of logistics—a significant component of modern business, involving the allocation and provision of supplies to meet needs—as part of an effort to supply imperial troops. Two centuries later, the concept of a postal service was introduced as Persian emperors sought to maintain communication with field commanders.

The Romans developed their roads, which ultimately provided the blueprint for the modern superhighway system—itsself a concept introduced in the 1950s by President Dwight D. Eisenhower with military needs in mind. In about 100 B.C., Chinese armies began using the wheelbarrow, a piece of technology so vital to the transport of military material that the emperor kept its design a secret for many years.

The list of military technological developments with civilian applications continues right up to the U.S. space program in the late twentieth century, without which modern satellite communication—to name just one example—would not be possible. Satellite technology, in turn, facilitated the military’s global positioning system (GPS), today used by civilians for navigation in onboard

vehicle systems. Additionally, the U.S. intelligence community and military played a pivotal role in developing the Internet.

### The Dual Use Science and Technology Program

In an effort to formalize the interaction between military and civilian technological innovations, DOD established the Dual Use Science and Technology (DU S&T) Program, through which it partners with industry. As DOD officials have noted, there can be commonalities of aim between the need to maintain U.S. technological superiority on the battlefield, and the competitive edge of U.S. industry in the marketplace.

In order to facilitate partnerships, DOD has sought to develop streamlined contracting procedures, and to implement cost sharing between its DU S&T Program, the military services, and industry. The benefits to industry inherent in these partnerships include the leveraging of scarce science and technology funds, access to advanced technology, and the means of developing further beneficial partnerships with other firms, defense laboratories, and university research departments.

In order to qualify as a DU S&T project, an undertaking must have a clearly demonstrable dual use potential, and at least half of the project cost must be underwritten by non-federal participants, of which at least one must be a for-profit company or corporation. Awarding must be based on competitive procedures in compliance with federal regulations for equal opportunity, and projects must meet DOD requirements regarding procurement.

**Benefits and risks.** A 1999 report in *Naval Forces* provided a number of examples of benefits to be reaped from dual-use programs involving technology developed by a single division of the U.S. Navy, the Naval Undersea Warfare Center (NUWC) in Newport, Rhode Island. During the late 1960s, defense contractor General Electric began developing laser-based listening technology for the detection of quiet-operating submarines at great distances deep beneath the ocean surface. Put on hold at the end of the Cold War, the project had received new life through a partnership between the NUWC Weapons Systems Directorate, Flight Safety Technologies, and Lockheed Martin.

The joint project would have applications for air safety by making it possible for pilots to detect hazards that do not show up on ordinary radar. Among these are the turbulence produced in the wake of large aircraft, forms of clear-air turbulence, wind shear, and microbursts, or sharp downdrafts produced in extreme weather conditions. Because these are not accompanied by rain or hail, radar cannot detect them, but much more discriminating laser beams are capable of “seeing” rather than “hearing” sounds, thus potentially providing advance warning of a disturbance that could cause a plane crash.

Undersea warfare (USW) also makes use of sonar, which could be applied in searching a mammogram x ray for minuscule abnormalities. Such was the focus of a program under development in a partnership between the NUWC Technology Transfer Program, the Weapons Systems Directorate, and the Faulkner Sagoff Center for Breast Health Care in Boston. Another promising partnership was a joint project with Precision Signal Incorporated of Boca Raton, Florida, to produce an imaging unit capable of detecting small objects buried under the sea floor. Called the Ocean Bottom Profiler, the device could be used to detect hazardous materials and other items that have sunk to the bottom of the ocean.

**The need for controls.** Great advances carry with them a number of potential risks, not least of which is the chance that military innovations may be stolen or appropriated by hostile powers. This reality came to the forefront in the late 1990s, as persons both inside and outside the ranks of the federal government became concerned over alleged efforts by the People's Republic of China to appropriate U.S. military technology for its own purposes. Similarly, concerns were raised as to the use of sophisticated technologies by terrorist groups or terror-sponsoring nations to develop weapons of mass destruction.

"In a perfect world," Commerce Department Undersecretary for Export Administration William Reinsch told reporters in January 1998, "I would have multilateral agreements that would require consensus" before sensitive technologies could be exported. As Reinsch noted, "Right now there is no veto [for the United States], but during the Cold War, if the French wanted to sell something to the Chinese, we could block it."

Reinsch, the senior government official responsible for issuing export licenses on dual-use technologies, was referring to a Cold War-era organization known as COCOM, or the Coordinating Committee for Multilateral Export Controls. When COCOM was in operation, its membership—composed of industrialized democracies—had to reach unanimous agreement before civil or military hardware could be exported to states such as the Soviet Union and the Warsaw Pact nations, China, Cuba, North

Korea, more aggressive states in the Middle East, and South Africa under the apartheid regime.

With the end of the Cold War, COCOM had disbanded, and no similar mechanism was in place. In lieu of such agreements, the United States and the nations of Western Europe relied on agreements of mutual consent, but these often broke down in the face of conflicting views as to the threat posed by certain nations. In the case of North Korea, most of the world's advanced nations agreed that it posed a threat, but when it came to Iran—a nation the United States accused of supporting terrorism—U.S. and European views differed. In order to prevent the illegal transfer of dual-use and other sensitive technologies to hostile nations, Reinsch called for an increased vigilance on the part of vendor companies, as well as the tasking of more U.S. agents to monitor potential transfers.

#### ■ FURTHER READING:

##### PERIODICALS:

Baus, Theresa. "Dual Use Technology." *Naval Forces* 20, no. 3 (1999): S54–S55.

Muradian, Vago. "Better Export Controls Needed to Check Dual-Use Technologies." *Defense Daily* 198, no. 14 (January 22, 1998): 1.

Palfrey, Terry. "The Hidden Legacy of Scott: Weapons of Mass Destruction and the UK Government Proposals to Control the Transfer of Technology by Intangible Means." *International Review of Law, Computers & Technology* 13, no. 2 (August 1999): 163–181.

Sharke, Paul. "The Start of a New Movement." *Mechanical Engineering* 124, no. 8 (August 2002): 47–49.

##### ELECTRONIC:

Dual Use Science and Technology Program. <<http://www.dtic.mil/dust/>> (April 14, 2003).

##### SEE ALSO

*Information Security*  
*Satellite Technology Exports to the People's Republic of China (PRC)*  
*Technology Transfer Center (NTTC), Emergency Response Technology Program*



*This page intentionally left blank*

# E

## E-2C

Built by Northrop Grumman and first used by the U.S. Navy in 1964, the E-2C Hawkeye has served as an airborne early warning and command and control aircraft in the

Vietnam and Persian Gulf wars, as well as in the war on drugs. It is also in service with five foreign governments. The most distinctive feature of the E-2C, which provides simultaneous air and surface surveillance, is its rotating 24-foot (7.3-m) radar dome above the fuselage.

The first airborne early warning and command and control aircraft was the Grumman E-1 Tracer, which flew



An E-2C “Hawkeye” surveillance plane assigned to the “Wallbangers” of the Carrier Airborne Early Warning Squadron taxis on the flight deck aboard USS *Carl Vinson* after completing a patrol, September 15, 2001. ©REUTERS NEWMEDIA INC./CORBIS.

from 1954 to 1964. In 1964, the navy phased in the E-2 Hawkeye, the first aircraft designed to be carrier-based and serve an all-weather airborne early warning and command and control function. Nine years later, in 1973, Grumman introduced the E-2C model. Over the next three decades, the E-2C underwent five major changes, with the fifth, known as Hawkeye 2000, introduced in October 2001.

Using computerized sensors to provide early warning, the E-2C is a high-wing aircraft whose rotating dome contains stacked antennae. The airflow over and around the dome necessitates the second most distinctive of its design features, a multiple-surface tail unit.

In addition to their service in Vietnam, Hawkeyes directed F-14 Tomcat fighters on combat air patrol during strikes against terrorist-related Libyan targets in 1986. They also directed both land attacks and combat air patrol missions over Iraq during the Persian Gulf War, providing control for the shootdown of two Iraqi MiG-21 fighter jets by carrier-based F/A-18s in the first days of the conflict.

E-2Cs have also served with the Drug Enforcement Administration and other law-enforcement agencies for the interdiction of smuggled drugs. The governments of Egypt, France, Japan, Singapore, and Taiwan have purchased E-2Cs, which are engineered in Bethpage, New York, and produced and modified in St. Augustine, Florida.

#### ■ FURTHER READING:

##### BOOKS:

Chant, Christopher. *An Illustrated Data Guide to Modern Reconnaissance Aircraft*. London: Tiger Books International, 1997.

Hardy, M. J. *Sea, Sky, and Stars: An Illustrated History of Grumman Aircraft*. New York: Sterling, 1987.

##### PERIODICALS:

Dietrich, Bill. "Engineering—Here's What You Can Expect Next Century." *Seattle Times*. (December 15, 1992): D1.

Wilson, George C. "Drug-War Radar Picks up a Funding Blip." *Washington Post*. (April 14, 1987): A21.

"Young Defends \$13 Billion CVN-21 Development Investment." *Defense Daily* 217, no. 32 (February 19, 2003): 1.

##### ELECTRONIC:

E-2C Hawkeye. United States Navy Fact File. <<http://www.chinfo.navy.mil/navpalib/factfile/aircraft/air-e2c.html>> (March 9, 2003).

##### SEE ALSO

J-STARS  
Persian Gulf War

## Ebola Virus

■ BRIAN D. HOYLE

The Ebola virus is one of two members of a family of viruses that is designated as the Filoviridae. The name of the virus comes from a river located in the Democratic Republic of the Congo, where the virus was discovered. Although naturally occurring, some public health experts worry that the lethality of the virus makes it an attractive potential bioterrorism agent. Under natural circumstances Ebola induced hemorrhagic fever carriers have such high death rates that their rapid death actually acts to limit the spread of the virus. Deliberate spread of the virus would counteract this natural limiting factor.

The species of Ebola virus are among a number of viruses that cause a disease, hemorrhagic fever, that is typified by copious internal bleeding and bleeding from various orifices of the body, including the eyes. The disease can be swiftly devastating and results in death in over 90 per cent of cases.

To date, four species of Ebola virus have been identified, based on differences in their genetic sequences and in the immune reaction they elicit in infected individuals. Three of the species cause disease in humans. These are Ebola-Zaire (isolated in 1976), Ebola-Sudan (also isolated in 1976), and Ebola-Ivory Coast (isolated in 1994). The fourth species, called Ebola-Reston, causes disease in primates. The latter species is capable of infecting humans but so far has not caused disease in humans. Ebola-Reston is named for the United States military primate research facility where the virus was isolated, during a 1989 outbreak of the disease caused by infected monkeys that had been imported from the Philippines. Until the non-human involvement of the disease was proven, the outbreak was thought to be the first outside of Africa.

The appearance of the Ebola virus only dates back to 1976. The explosive onset of the illness and the underdeveloped and wild nature of the African region of the virus's appearance have complicated the definitive determinations of the origin and natural habitat of Ebola. The source of the Ebola virus is still unknown. However, given that filovirus, which produce similar effects, establish a latent infection in African monkeys, macaques, and chimpanzees, scientists consider the possibility that the Ebola virus likewise normally resides in an animal that lives in Africa. A search for Ebola virus in such primates has so far not revealed evidence of the virus.

Almost all confirmed cases of Ebola from 1976 to 2002 have been in Africa. In the latest outbreak, which has been ongoing since late in 2001, 54 people have died in the Gabon as of February of 2002. In the past, one individual in Liberia presented immunological evidence of exposure to Ebola, but had no symptoms. As well, a laboratory worker

in England developed Ebola fever as a result of a laboratory accident in which the worker was punctured by an Ebola-containing needle.

The Ebola virus produces a high fever, headache, muscle aches, abdominal pain, tiredness and diarrhea within a few days after infecting a person. Some people will also display bloody diarrhea and vomit blood. At this stage of the disease some people recover. But, for most of those who are infected, the disease progresses within days to produce copious internal bleeding, shock and death.

Outbreaks of infection with the Ebola virus appear sporadically and suddenly. The outbreak rapidly moves through the local population and often just as quickly ends. The initial infection is presumable by contact between the person and the animal that harbors the virus. Subsequent person-to-person spread likely occurs by contamination with the infected blood or body tissues of an infected person in the home or hospital setting, or via contaminated needles. The fact that infected people tend to be in more under-developed regions, where even the health care facilities are not as likely to be equipped with isolation wards, furthers the risk of spread. The person-to-person passage is immediate; unlike the animal host, people do not harbor the virus for lengthy periods of time.

The possibility of air-borne transmission of the virus is debatable. Ebola-Reston may well have been transmitted from monkey to monkey in the Reston military facility via the air distribution system, since some of the monkeys that were infected were never in physical contact with the other infected monkeys. However, if the other species of the virus are capable of similar transmission, this has not yet been documented. Laboratory studies have shown that Ebola virus can remain infectious when aerosolized. But the current consensus is that airborne transmission is possible but plays a minor role in the spread of the virus.

In the intervening years between the sporadic outbreaks, the Ebola virus probably is resident in the natural reservoir.

Currently there is no cure for the infection caused by the Ebola virus. However, near the end of an outbreak of the virus in 1995 in Kikwit, Africa, blood products from survivors of the infection were transfused into those actively experiencing the disease. Of those eight people who received the blood, only one person died. Whether or not the transfused blood conveyed protective factor was not ascertained. A detailed examination of this possibility awaits another outbreak.

The molecular basis for the establishment of an infection by the Ebola virus is still also more in the realm of proposal than fact. One clue has been the finding of a glycoprotein that is a shortened version of the viral constituent in the circulating fluid of humans and monkeys. This protein has been suggested to function as a decoy for the immune system, diverting the immune defenses from the actual site of viral infection. Another

immunosuppressive mechanism may be the selective invasion and damage of the spleen and the lymph nodes, which are vital in the functioning of the immune system.

The devastating infection caused by the Ebola virus is all the more remarkable given the very small size of the viral genome, or complement of genetic material. Fewer than a dozen genes have been detected. How the virus establishes an infection and evades the host immune system with only the capacity to code for less than twelve proteins is unknown.

#### ■ FURTHER READING:

##### BOOKS:

Cormican, M. G. and M. A. Pfaller. "Molecular Pathology of Infectious Diseases," in *Clinical Diagnosis and Management by Laboratory Methods*, 20th ed. Philadelphia: W. B. Saunders, 2001.

##### PERIODICALS:

Peters, C. J., and J. W. LeDuc. "An Introduction to Ebola: The Virus and the Disease." *The Journal of Infectious Diseases* no. 179 (Supplement 1, February 1999): ix-xvi.

##### ELECTRONIC:

Centers for Disease Control. "Ebola Hemorrhagic Fever." 2001. <<http://www.cdc.gov/ncidod/dvrd/spb/mnpages/dispages/ebola.htm>> (March 12, 2003).

———. "Viral Hemorrhagic Fevers." 2000. <<http://www.cdc.gov/ncidod/dvrd/spb/mnpages/dispages/vhf.htm>> (March 12, 2003).

##### SEE ALSO

*Biological Warfare*  
*Biological Weapons, Genetic Identification*  
*Bioshield Project*  
*Bioterrorism*  
*CDC (United States Centers for Disease Control and Prevention)*  
*Hemorrhagic Fevers and Diseases*  
*Viral Biology*

---

## E-Bomb

---

An e-bomb, or electronic bomb, is a non-explosive artillery shell that sends out an electromagnetic pulse (EMP) of enormous power, capable of permanently disabling mechanical and electronic systems. The concept developed in the 1920s, and was later recognized as an unintended consequence of nuclear explosions. By the beginning of the twenty-first century, United States and British scientists had the technology to develop e-bombs. At the same time, some observers warned that terrorists might be capable of building their own, much less sophisticated, devices for a fraction of the cost to a superpower.

Carbon-graphite coils capable of generating an electromagnetic pulse used to destroy electronics equipment—especially communications equipment—can be fitted to cruise missiles. Carbon-graphite equipped cruise missiles were used by U.S.-led forces in raids on Baghdad, Iraq in 1991 and in 2003.

**The Compton Effect and its consequences.** In 1925, American physicist and future Nobel laureate Arthur H. Compton demonstrated that when a string of subatomic energy packets called photons were fired into atoms with a low atomic number—that is, atoms with a relatively small number of protons in their nuclei—the atoms would eject electrons. This phenomenon, known as the Compton effect, is the principle underlying the e-bomb. If enough atoms eject enough electrons, which have a negative electric charge, the result is a massive electromagnetic pulse.

In 1958, when the United States conducted nuclear tests high above the Pacific Ocean, the explosions sent out bursts of gamma rays, extremely high-frequency electromagnetic waves. These collided with nitrogen and oxygen, which are the two most abundant elements in the atmosphere, and which both have very low atomic numbers—7 and 8 respectively. The result was an electromagnetic event whose effects were felt thousands of miles away. Street lights in Hawaii were blown out, and radio navigation as far away as Australia was interrupted for up to 18 hours.

Recognizing that these powerful EMPs were a by-product of nuclear explosions, American and allied scientists set out to harden the defenses of U.S. and NATO (North Atlantic Treaty Organization) electronic systems against disruption from nuclear explosions. Still, as long as the threat of thermonuclear exchange remained real during the Cold War, the EMPs themselves seemed a relatively insignificant side-effect of nuclear explosions.

**Developing e-bombs for the modern battlefield.** After the Cold War ended, physicists began to explore the use of EMPs as a high-tech weapon to yield a low-tech result: the complete devastation of an enemy's engines, telecommunications, and electronic systems by means of vast energy surges that, by overloading those systems, would render them permanently inoperable. Alarmed by news of Russian advances in the development of an e-bomb in 1998, Western scientists stepped up efforts to create their own e-bomb technology.

In 2000, British scientists announced the development of an e-bomb that could be fired from a long-range 155 mm. artillery gun or multiple-launch rocket system. U.S. scientists developed their own version, which was ready for use in the 2003 mobilization against Iraq. Military leaders leaned against using it, however, precisely because of the bomb's capabilities such as demobilizing hospitals and emergency services. Furthermore, in rebuilding an economy, the devastation of infrastructure

caused by an e-bomb could create prohibitive costs. However, for a terrorist organization less concerned with moral and practical compunctions, an e-bomb could be an attractive tool for creating vast destruction at a low cost.

#### ■ FURTHER READING:

##### PERIODICALS:

- Jenkins, Sally. "Peaceful Games, Cold War Sentiment." *Washington Post*. (February 25, 2002): D1.
- Sample, Ian. "Just a Normal Town...." *New Scientist* 167, no. 2245 (July 1, 2000): 20.
- Squeo, Anne Marie. "Leading the News: U.S. Studies Using 'E-Bomb' in Iraq—Electromagnetic Weapon Can Permanently Damage Telecom, Power Systems." *Wall Street Journal*. (February 20, 2003): A3.
- Wilson, Jim. "E-Bomb." *Popular Mechanics* 178, no. 9 (September 2001): 50–53.

##### SEE ALSO

*Electronic Warfare*  
*Microwave Weaponry, High Power (HPM)*

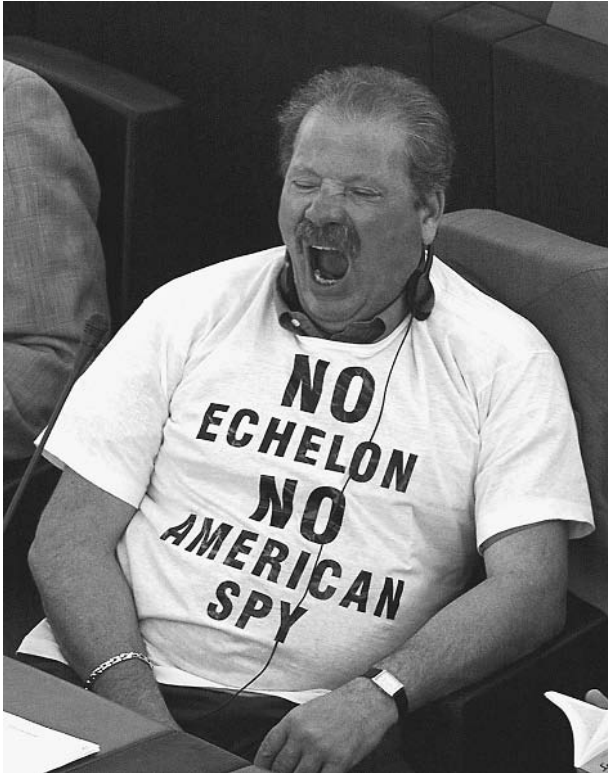
---

## Echelon

---

Echelon is the name for a global surveillance network consisting of ground stations, satellites, and other listening posts, which collectively intercept and analyze worldwide electronic communications. The signals intelligence agencies of five nations—the National Security Agency (NSA) of the United States, the Government Communications Headquarters (GCHQ) of the United Kingdom, the Communications Security Establishment (CSE) of Canada, the Defense Signals Directorate (DSD) of Australia, and the Government Communications and Security Bureau (GCSB) of New Zealand—all participate, with NSA as the controlling agency. Beginning in 1998, the governments of the European continent expressed increasing outrage over Echelon. However, their efforts to monitor their own citizens' communications suggest that this anger is not so much because Echelon exists at all, but because it is not under European control.

In 1943, the United States and United Kingdom signed the Brusa (British-U.S.A.) Agreement, which established a framework for the exchange of signals intelligence (SIGINT) between the two nations. Three years later, with the war over, the two signed the UKUSA (U.K.-U.S.A.) agreement of March 5, 1946, which brought together then SIGINT efforts of British, American, Canadian, Australian, and New Zealand intelligence. Each UKUSA nation had its own geographic spheres of influence, matched with its listening posts in certain parts of the globe, but the most powerful of the five nations—the United States—remained the unquestioned first among equals. In later years, a



Italian Eurodeputy Roberto Felice Bigliardo wears a t-shirt protesting against the U.S. communications surveillance system Echelon during debates in the European parliament in Strasbourg 05 July 2000. ©AFP/CORBIS.

number of other countries, including Denmark, Germany, Norway, and Turkey, signed “third-party” agreements of participation in the UKUSA network.

Over the years, there emerged a network of listening posts and satellites intercepting cables, telephone communications, radio and microwave signals, wireless communications, e-mail, faxes, and other forms of communication traffic. Almost nothing was immune from the system that came to be known as Echelon, whether a telegram sending birthday greetings to a child in Great Britain, or walkie-talkie communications between East German guards on the Berlin Wall. UKUSA participants were forbidden by law from intercepting communications that originate and terminate in their own countries, but the exchange of information between intelligence services effectively rendered these prohibitions moot. Perhaps NSA, for instance, could not monitor communications within the United States, but GCHQ could with impunity, and it was a simple matter to pass this information on to NSA.

The Echelon system seems to have emerged in something like its present form, though at a much less advanced technological stage, during the early 1970s. In the late 1960s, as NSA and GCHQ geared up for the use of satellites on a grand scale, U.S. and British leadership began to recognize the need for interception and processing sites. The first ground station in what came to be known as

Echelon was established at Morwenstow, Cornwall, in England, using two large dish antennae to intercept communications across the Atlantic and Indian oceans. Soon NSA built another such station at Yakima, Washington, to intercept communications across the Pacific. Other sites followed, among them Menwith Hill in England, Stanley Bay in Hong Kong (dismantled and moved to Australia prior to the Chinese takeover in 1997), and Sugar Grove in West Virginia.

**The technology of Echelon.** Echelon has its own security compartments: SECRET SPOKE instead of CONFIDENTIAL, UMBRA GAMMA instead of SECRET, and TOP SECRET UMBRA instead of TOP SECRET, a compartment that it trumps for level of secrecy and security classification. Echelon also long ago developed its own wide-area network (WAN), much like the public Internet today, only this network is completely inaccessible to public traffic.

The Echelon wide-area network includes an intelligence news network known as Newsdealer, a TV conference system called Giggle, and other components. E-mail and Web pages have an appearance very much like those of their counterparts in the ordinary world, but again, the similarity ends at the superficial resemblance. Through a system known as Intelink, analysts can browse pages on NSA’s server and select specific geographic areas from which to obtain products ranging from video clips and satellite photos to intelligence and status reports, as well as databases.

**Dictionaries.** As the targets of Echelon eavesdropping have evolved—from cable traffic and land-line telecommunications to cell-phone traffic and e-mails—so have its tools. These include not only satellites, but also computers for filtering traffic to extract relevant data.

Once this was a painstaking process, with analysts surveying reams of sheets by hand, marking them for specific items of intelligence. Today, computers do most of this work, thanks to systems known as dictionaries—a computer programmed to scan data for specific terms and keywords.

Echelon dictionary computers around the world scan the traffic under their purview, not only for their own keywords, but also for those of other agencies. In time, keyword searches may be replaced by the more efficient method of topic analysis, which employs principles similar to those of “fuzzy logic” in an effort to better replicate the selection process that the human itself undergoes, albeit at a much slower rate.

**Outrage over Echelon.** It has been estimated that for a million inputs (a single phone call being an example of an input), Echelon’s dictionaries eliminate all but 6,500 as unimportant. Of these, only 1,000 meet the criteria for forwarding them to analysts, who typically select only 10 for closer

study. From these 10, only one warrants the production of an intelligence report. These statistics tend to suggest that, though civil libertarians and others may be outraged over the existence of a system such as Echelon, NSA is really not interested in listening in on most people's phone conversations. It simply sifts through 99.9999 percent of the communication taking place in the world at any given time so as to winnow out the 0.0001 percent that warrants its attention.

Still, concerns about Echelon motivated Margaret "Peg" Newsham, a former computer systems analyst, to release the first reports about the system in 1988. During the early 1990s, New Zealand journalist Nicky Hager painstakingly researched the system to produce his 1996 book *Secret Power*, and in the late 1990s, respected U.S. intelligence writer Jeff Richelson studied Echelon. The European Union also published a report on Echelon in 2001, in which it called on European citizens to encrypt their e-mails as a means of protecting them from snooping by the intelligence services of the English-speaking countries. At the same time, the European Union was considering proposals to require Internet service providers and telecommunications companies to record all their customers' communications and archive them for at least a year—a measure that suggests the UKUSA countries do not have the monopoly on snooping in the liberal democratic world, much less in the world as a whole.

#### ■ FURTHER READING:

##### BOOKS:

- Bennett, Richard M. *Espionage: An Encyclopedia of Spies and Secrets*. London: Virgin Books, 2002.
- Best, Richard A. *Project Echelon: U.S. Electronic Surveillance Efforts*. Washington, D.C.: Congressional Research Service, 2000.
- Hager, Nicky. *Secret Power*. Nelson, New Zealand: Craig Potton, 1996.
- Richelson, Jeffrey T. *The U.S. Intelligence Community*, fourth edition. Boulder, CO: Westview Press, 1999.

##### PERIODICALS:

- Auer, Catherine. "EU Knocks Echelon, Wants Own Super Spy." *Bulletin of the Atomic Scientists* 57, no. 5 (September/October 2001): 11.
- Evers, Joris. "U.S. Spy Technology Failed to Signal Attack Planning." *InfoWorld* 23, no. 38 (September 17, 2001): 28.
- Melloan, George. "Civil Liberties Give Way to the Search for Terrorists." *Wall Street Journal*. (October 23, 2001): A27.
- Poole, Patrick. "'Echelon' Spells Trouble for Global Communications." *Privacy Journal* 25, no. 11 (September 1999): 3–4.

##### ELECTRONIC:

- Campbell, Duncan. Inside Echelon. <<http://www.heise.de/tp/english/inhalt/te/6929/1.html>> (March 24, 2003).

Easton, Gary. British Broadcasting Corporation News. <<http://news.bbc.co.uk/1/h1/world/americas/1577313.stm>> (March 24, 2003).

#### SEE ALSO

*COMINT (Communications Intelligence)*  
*Information Warfare*  
*NSA (United States National Security Agency)*  
*Satellites, Spy*  
*Security Clearance Investigations*  
*SIGINT (Signals Intelligence)*  
*Special Relationship: Technology Sharing Between the Intelligence Agencies of the United States and United Kingdom*  
*United Kingdom, Intelligence and Security*

## Economic Espionage

#### ■ JUDSON KNIGHT

Economic espionage, sometimes known as industrial espionage, is spying conducted for the benefit of a commercial or industrial enterprise, typically to gain information not available through open channels. (By contrast, economic intelligence conducted on behalf of governments usually draws on information available through open channels.) Technologically advanced nations such as the United States are most vulnerable to economic espionage, which threatens hundreds of billions of dollars in U.S. economic losses to industry. In an attempt to curb industrial and commercial spying, Congress in 1996 passed the Economic Espionage Act, but challenges to U.S. companies have continued.

**Vulnerabilities.** According to a 1999 report delivered by the American Society for Industrial Security (ASIS) to the Federal Bureau of Investigation (FBI), some \$300 billion worth of U.S. intellectual property was directly threatened by industrial espionage in 1997 alone. The ASIS noted more than 270 individual cases of theft and attempted theft involving commercial information. In 2000, the ASIS estimated that each year, losses and potential losses from economic espionage cost American industry more than \$60 billion each year. Of 1,300 companies surveyed by the ASIS, fully 1,100 reported that they had been the targets of economic espionage.

Just as the most highly industrialized nations are the obvious potential victims of economic espionage, emerging industrial powers and their economic firms are often the most likely perpetrators. Such is the case with China, which figured in a number of news reports involving economic espionage during the 1990s and early 2000s.

In November, 2001, for instance, the FBI learned of an attempt by individuals operating a Chinese corporation to



Pen Yen Yang, pictured, was among the first to be convicted of economic espionage under the Economic Espionage Act of 1996, which banned the theft of trade secrets. AP/WIDE WORLD PHOTOS.

steal information from Transmeta, a computer hardware company in California's Silicon Valley. According to an affidavit submitted by the FBI to the U.S. District Court in San Jose, Transmeta employee Fei Ye had partnered with fellow Chinese nationals Sun Li and Ming Zhong in a company called Supervision Incorporated. Backing the company, created to develop high-speed, high-performance computer processors, was the Chinese government, according to the FBI.

America is certainly not the only victim of economic espionage. In 2003, for instance, Swedish authorities expelled two Russian diplomats accused of spying at Ericsson, a manufacturer of radar and missile-guidance systems for Sweden's principal strike warplane, the Gripen fighter jet. Nor are the nations involved in spying always inferior technological powers, such as Russia or China; the United States has on several occasions been the target of economic espionage by high-quality producers of technology, including Japan, France, and Israel.

**Spying by technological competitors.** Despite the close relationship between the United States and Japan in matters of national defense, the Central Intelligence Agency (CIA) estimated in 1987 that 80 percent of Japanese intelligence-gathering activities were directed toward U.S. industry, particularly in high-tech and computer-related fields.

U.S. military contractor Recon/Optical in 1992 accused Israel of attempting to appropriate a design for an airborne spy camera, and after lengthy legal wranglings, the Israelis agreed to settle out of court.

In 1993, the CIA warned U.S. aircraft manufacturers to be on the lookout for French spies at the Paris Air Show, and intelligence officials have claimed that France regularly sponsors the theft of information from U.S. companies. A French intelligence official defended his country's efforts in economic espionage with a public statement to the effect that spying in the modern world is primarily directed toward "economic, scientific, technological, and financial" objectives.

**U.S. spying.** Responding to these and other accusations, the French in 1995 accused a CIA operative of attempting to obtain classified information from an official of their government. Under the leadership of Admiral Stansfield Turner in the late 1970s and early 1980s, the CIA regularly sponsored Commerce Department briefings at which U.S. corporate executives received information on developments in semiconductor and aircraft technology by foreign powers. American authorities continued to deny the French charges in the mid-1990s. For the most part, the leading technology is in America. While U.S. intelligence has a powerful motivation to keep tabs on the activities of foreign technological concerns, the purpose is primarily defensive, because the United States and its companies have less to gain by stealing from overseas.

**Protecting U.S. technology.** By the same token, U.S. companies are vulnerable to foreign competitors—and to one another. For this reason, the federal government has put in place a number of mechanisms to protect American industry. One of these is the CIA, which monitors potential cases of economic espionage against U.S. companies by foreign concerns. If the CIA uncovers information regarding possible criminal activity such as bribery, it turns this over to the FBI. Additionally, the National Security Agency (NSA), despite the high levels of secrecy involving its activities, sometimes passes on information to the FBI, which notifies threatened companies using documentation that leaves out sensitive NSA information.

The Office of the National Counterintelligence Executive (NCIX), formerly known as the National Counterintelligence Center (NACIC), coordinates and distributes information on economic espionage gained by intelligence. NCIX distributes this information to targeted U.S. companies on an as-needed basis. The U.S. State Department monitors information on economic espionage through its Bureau of Intelligence and Research (INR), and keeps U.S. companies informed of threats by means of its Overseas Security Advisory Council electronic bulletin board.

To provide further protections for U.S. companies, Congress in 1996 passed, and President William J. Clinton



signed into law, the Economic Espionage Act. The act makes it a federal crime to use unauthorized means to obtain any trade secret whose transfer to other parties would cause economic harm to its lawful owner. "Unauthorized means" include the use of undercover employees, pretexts, and the development of confidential informants in order to obtain trade secrets. The act does not address the gathering of information through open sources.

Despite the many efforts of the federal government to protect sensitive trade, industrial, and commercial information, the first and often the best line of defense still lies with the company itself. In order to protect assets from economic espionage, a 2003 report in *Security* recommended that employees be educated, and technology implemented, so as to track proprietary information. The report also recommended a "cultural approach" to security, meaning that companies should recognize the leading role played by people and processes, and not simply address information and facility security from a technological standpoint.

To better protect against economic espionage, according to the *Security* report, a number of steps must be taken, beginning with the often-overlooked measure of conducting an evaluation. During this process, company security personnel should review work practices, identify the most sensitive compartments of information, and note the points and areas at which allegedly secure information is transferred. The company should invest in security technology only after this review, which will assist it in best targeting funds for security.

#### ■ FURTHER READING:

##### PERIODICALS:

Carr, Chris, Jerry Furniss, and Jack Morton. "Complying with the Economic Espionage Act." *Risk Management* 47, no. 3 (March 2000): 21–24.

Jeffrey, Terence P. "Two Silicon Valley Engineers Indicted for Economic Espionage Aiding China." *Human Events* 59, no. 2 (January 13, 2003): 1.

Joyce, Jim. "Espionage Battleground." *Security* 40, no. 1 (January 2003): 24–25.

Nasheri, Hedieh, and Timothy J. O'Hearn. "High-Tech Crimes and the American Economic Machine." *International Review of Law, Computers & Technology* 13, no. 1 (March 1999): 7–19.

Wolkowitz, Dave. "Facility Security—Playing It Safe." *Area Development Site and Facility Planning* 37, no. 9 (September 2002): 72.

##### SEE ALSO

*Chinese Espionage Against the United States Counter-Intelligence Economic Intelligence Facility Security NCIX (National Counterintelligence Executive), United States Office of the Satellite Technology Exports to the People's Republic of China (PRC) Technical Intelligence*

## Economic Intelligence

■ MARTIN J. MANNING

Economic intelligence can be loosely defined as information gathered about materials and resources that are developed, produced, or managed outside the United States, and the interpretation and presentation of raw information or unpublished data to reports or analyses that inform policy makers and consumers.

**Background.** The importance of economic intelligence first surfaced in 1776 when the Committee of Secret Correspondence of the Continental Congress, considered the first U.S. intelligence agency, sent William Carmichael to Europe to survey several economic matters crucial to the emerging government, such as foreign competition in European markets from tobacco grown in the Ukrainian provinces of the Russian Empire. In his secret dispatch (November 1776) from Amsterdam, Carmichael reassured his superiors that, despite the fears that "the Ukraine would supply Europe with tobacco," the best that he saw "is worse than the worst of our ground leaf."

During World War I, an economic intelligence section, within the Army's military intelligence operation, was headed by a future U.S. Secretary of State John Foster Dulles. When this war ended, and President Wilson was preparing for the Versailles Peace Conference, he consulted private experts, the "Inquiry," which gathered economic intelligence from its headquarters at the American Geographical Society, New York.

In World War II, U.S. government agencies, such as the Board of Economic Warfare, studied the Japanese economy while the Office of Strategic Services (OSS) collected information on key commodities, including tungsten; its Russian division, directed by economic experts Abram Bergson and Wassily Leontief, targeted appraisals of the Soviet Union's postwar economic condition.

**Post-World War II.** In 1945, OSS was abolished; its successor, Central Intelligence Group (CIG), coordinated economic intelligence. Its June 1946 report gathered intelligence on foreign industrial establishments and foreign petroleum extraction, compiled comprehensive geographic information, and utilized the services of its foreign officers to gather data on strategic minerals.

When the Central Intelligence Agency (CIA) was established as part of the National Security Act of 1947, its role to monitor national intelligence, by coordinating the information collected by the various departments of government, was supplemented by a 1949 recommendation of a review group that the CIA create an Office of Research Reports (ORR) to collect and examine economic information.

In National Security Council Intelligence Directive No. 15, *Coordination and Production of Foreign Economic Intelligence* (June 13, 1951), CIA was given responsibility to determine the overall requirements of foreign economic intelligence, to evaluate foreign economic data of significance to national security issues, and to conduct “such foreign economic research and produce such foreign economic intelligence” as required to supplement work being done by other agencies. A year later, Director of Central Intelligence, Walter B. Smith, informed the NSC that the ORR was releasing accurate appraisals of an “enemy’s economic potential” and that an interdepartmental Economic Intelligence Committee to establish priorities and publish interdepartmental economic estimates, was in place, chaired by the ORR assistant director.

The allocation of responsibility for economic intelligence over the next 20 years shifted between the CIA and the Department of State. Both worked closely together during the Truman administration when the State Department produced economic intelligence on countries outside the Sino-Soviet Bloc while CIA compiled economic intelligence on the Sino-Soviet Bloc. By 1955, the CIA Office of Research Reports was generally credited with composing the first good pictures of Soviet economic capabilities, including its transport system, current production, and plant capability. This analysis was relied upon by the Kennedy administration.

During the 1960s, the CIA became the government’s leading provider of economic intelligence as it expanded its economic analysis to “Free World” economies, especially to examine Soviet bloc economic activity in the developing world. After State’s Bureau of Intelligence and Research, hurt by shrinking budgets, cut the majority of its economic research to maintain its expertise for political analysis, CIA supplied regular economic inputs to national intelligence documents and picked up substantial new demands from policy makers, especially for information on developing countries.

By 1968, the CIA replaced ORR with the Office of Economic Research but the CIA’s overall importance in the provision of economic intelligence lessened during the Reagan Administration for several reasons: the U.S. Department of the Treasury and the Federal Reserve Board improved their monitoring of international financial issues; new competition came from the highly sophisticated technology of international economic analysis available from the private sector; the international financial institutions, such as the International Monetary Fund (IMF) and the World Bank, supplied their own economic expertise; and a variety of on-line services, newspapers and trade publications made a vast amount of data available to non-government subscribers.

The exact role of economic intelligence remains a widely debated issue. According to Dr. Mark Lowenthal, Senior Specialist in U.S. Foreign Policy, Congressional Research Service, Library of Congress, in testimony before the U.S. Senate’s Select Committee on Intelligence,

August 5, 1993, no one questions the importance of economic issues but there is “no broad consensus” about the Intelligence Community’s proper role in it. He noted that the issue has been oversimplified by calls for “more economic intelligence” unsupported by any “knowledge of long standing activities in that area or of the likely utility of these intelligence activities and products to economic problems or issues.” Lowenthal argues that no persuasive case has yet been made that “U.S. economic competitiveness requires large-scale aid from the Intelligence Community.”

**Types of information.** There are three main sources of economic intelligence. The first, open sources, range from official statistical publications, newspapers, radio broadcasts, and trade publications to IMF country studies. Unclassified sources generally constitute the foundation of any economic analysis, an interpretation of the overall picture.

The second are the reports and cables from U.S. embassies and consulates, compiled by State Department economic officers, Treasury Department attachés, and officers of the Foreign Commercial Service.

The third, clandestine information, is obtained without either the knowledge or consent of foreign governments. It can come from satellites, from intercepted communications, or from secrets stolen by a foreign national employed by the United States.

**Present situation.** The CIA, assisted by other government agencies, provides economic intelligence for U.S. policy, with experts monitoring international transactions (including sanctions enforcement and illicit finance); international economic and environmental problems, including trade and finance; defense markets and logistics; geographic resources, including demographics and commodities; civil technology, including aerospace, advanced manufacturing, and emerging technologies; and energy resources. However, critics feel that American companies don’t need the CIA to compete in the global marketplace. The glut of information (sometimes too much information) coming from the Internet, private citizens, groups and organizations with access to foreign economic activities, and subscriber services, such as *The Economist’s* Economic Intelligence Unit (EIU) databases, complement and sometimes replace official channels.

**Resources.** The official record of economic intelligence in U.S. economic diplomacy is in the Foreign Relations of the United States series volumes compiled by the Office of the Historian, U.S. Department of State; published by the Government Printing Office. Beginning with 1944: vol. II; *General: Economic and Social Matters* (Washington: GPO, 1967), individual volumes have dealt with U.S. economic policy.

An excellent introduction to the history of U.S. economic intelligence is: Philip Zelikow, "American Economic Intelligence: Past Practice and Future Principles," *Intelligence and National Security* 12, no. 1 (January 1997):164–177. I am indebted to Mr. Zelikow's research for providing background for this essay.

#### ■ FURTHER READING:

##### BOOKS:

Katz, Barry M. *Foreign Intelligence and Research and Analysis in the Office of Strategic Services, 1942–1945*. Cambridge, MA: Harvard University, 1989.

U.S. Congress. Senate. Select Committee on Intelligence. *Economic Intelligence. Hearing, 103d Congress, 1st Session*. Washington, D.C.: GPO, 1994.

##### PERIODICALS:

Ernst, Maurice. "Economic Intelligence in CIA," *Studies in Intelligence* 28, no. 4 (Winter 1984): 1–16.

##### SEE ALSO

*Economic Espionage*

many Western intelligence and security efforts in North Africa and the Middle East. The rise of Islamist sects and terrorist groups in the region, as well as Egypt's close ties to neighboring Arab states, creates further diplomatic tensions with Europe and the United States. Although Egyptian intelligence agencies aided the United States intelligence community by providing information about the Al-Qaeda terrorist network, many in the Egyptian government opposed the United States led war in Afghanistan in 2001. Regardless, Egypt continues a liberal-use policy of its territorial waters for international shipping, including access to the Suez Canal.

The Egyptian Constitution prohibits religious political parties, but over the past decade, a few Islamist militant organizations have gained some political ground. In the 1990s, Egyptian and United States intelligence forces conducted operations to locate and capture Egyptian militants who had fled the country and were basing possible anti-government and terrorist operations abroad. The two nations successfully captured several suspects, but the Egyptian government garnered international criticism for human rights abuses, including poor treatment of the prisoners and the use of secretive military tribunals.

##### SEE ALSO

*Enduring Freedom, Operation Terrorism, Intelligence Based Threat and Risk Assessments*

## Egypt, Intelligence and Security

Egypt's primary intelligence agency is the General Directorate for State Security Investigations (GDSSI). The Ministry of the Interior administers the GDSSI. The agency collects both foreign and domestic intelligence, using civilian and military operatives and resources. The GDSSI maintains several operational departments and partner agencies, including the Counterintelligence Branch, the Department for Combating Religious Activity, Directorate of State Security Investigations, and a security action unit. The agency cooperates with military and foreign intelligence services in operations intended to protect national interests, especially relating to shipping, oil production, and refinement, and regional anti-terrorism measures. The organization has received criticism from human rights groups and members of the international community for its employment of harsh coercion techniques and conducting espionage on Egyptian citizens.

The government and the individual branches of service coordinate military intelligence. The organization assesses threats to national targets and actively protects military installations. Operations of the Intelligence Agency are classified.

While Egypt has cooperated with European and American anti-terrorist operations in the past, a recent political shift has prompted Egyptian authorities to withdraw from

## Eichmann, Adolf: Israeli Capture

■ ADRIENNE WILMOTH LERNER

Karl Adolf Eichmann (1906–1962) was the head of the German Gestapo Department of Jewish Affairs from 1941 to 1945. During World War II, Eichmann oversaw the deportation of European Jews to ghettos. In 1942, he organized the Wannsee Conference, a meeting of Nazi officials to devise the "Final Solution," the Nazi euphemism for the extermination of European Jews. Eichmann supervised the creation and operation of death camps, and set Nazi policy on the seizure of Jewish property. Immediately following the war, he was identified as one of the primary Nazi war criminals sought by international law enforcement and intelligence agencies.

After his arrest and escape from an American internment camp in 1946, Eichmann assumed a variety of pseudonyms and moved throughout Europe, never contacting his family. British and American intelligence searched for Eichmann for a few months, but as the Nuremberg Trials of other Nazi war criminals began, the focus of attention shifted from Eichmann and other escapees. The onset of



German Gestapo officer Adolf Eichmann listens to the guilty verdict read by the presiding judge as he stands in a bullet-proof glass enclosure in a Jerusalem court in 1961, during his trial for committing wartime atrocities against Jewish Europeans. AP/WIDE WORLD PHOTOS.

the Cold War further distracted the hunt for Nazi fugitives. Eichmann hid throughout Europe until 1950, before fleeing to Argentina with the aid of Nazi sympathizers. Once in South America, Eichmann sent for his family to join him. They eluded the authorities in Britain, Germany, and Israel who continued the search for various perpetrators of the Holocaust. It was through clues left by Eichmann's family, namely his sons Nikolas and Dieter, that authorities finally located Eichmann.

**Finding Eichmann.** During this time, Eichmann lived under the false name of Ricardo Klement, which he had taken when he escaped Europe. His sons, however, sometimes used the family name of Eichmann. In 1957, Eichmann's son Nikolas became involved with an Argentinean girl named Sylvia. Not knowing that the girl was Jewish, Nikolas often made anti-Semitic remarks and boasted of his father's deeds during the war. Nickolas' remarks, coupled with the occasional use of his real last name, made the girl's father suspicious. He contacted a friend in Germany, jurist Fritz Bauer. Bauer, who was imprisoned by the Nazis twice during the war, devoted his life to the location and capture of Nazi war criminals. Bauer notified Israeli authorities with the information.

Though Israel was a new nation, it had already developed a skilled intelligence service. A special unit of that service was called Mossad. The unit was formed to track down and kill enemies of the state, but dedicated its first few decades to the capture of terrorists and war criminals. The head of Mossad, Isser Harel, immediately took charge of the hunt for Eichmann. He chose a special team of 30 agents, several of them survivors of the Holocaust, to assist in the operation. The Israeli government decided that Eichmann should not be assassinated, but brought back to Israel to stand trial. To further complicate the matter, once Eichmann was found, he would have to be kidnapped and smuggled to Israel, a violation of Argentinean legal sovereignty. Because many Nazi sympathizers found refuge in South America during the war, the Israelis knew that a diplomatic extradition would be difficult, if not impossible, to obtain.

The lead that Bauer gave Mossad turned into a dead end. When an agent tried to locate the family, he discovered that Eichmann and his family had moved, with no forwarding address. Another lead surfaced in 1959. One of Bauer's informants in Italy discovered the pseudonym that Eichmann used when he immigrated to South America. Another agent discovered that a gas meter on the house from the first tip still bore the name Klement. Authorities were convinced that the man was Eichmann.

Mossad hatched a simple plan to find Eichmann's new address. Around the time of Nikolas' birthday, Mossad hired an undercover agent to dress as a bellboy and approach Dieter Eichmann with a package that needed to be delivered to his brother, Nikolas. The undercover agent did not know anything else about the mission. Dieter refused to give the bellboy his brother's address, and took the package himself. Prepared for this outcome, the Mossad team sent the undercover agent back to Dieter a few days later. The agent told Dieter that the sender of the package believed that the package was not delivered and demanded that she be paid for its lost contents. Dieter claimed that the package was not delivered to Nikolas because he was confused about the name, Nikolas Klement, which appeared on the box. Dieter further explained that his brother used the surname Eichmann, so he thought the package belonged to his father, Ricardo Klement. Dieter then reluctantly gave the bellboy his father's address, 14, Garibaldi Street, San Fernando. Mossad agents watched the house for several weeks, tracking Eichmann's daily schedule. One evening, the subject believed to be Eichmann stepped off his usual bus carrying flowers. He was greeted at his home by several people who gathered for a party. The day corresponded with Eichmann's wedding anniversary. These facts convinced the Mossad agents that they had positively identified the subject as Adolf Eichmann.

**Eichmann's Capture.** After locating Eichmann, agents then devised a plan for his capture and kidnapping. The Israeli team saw an opportunity to ferry Eichmann out of the country during the upcoming celebration of Argentina's

100th anniversary of independence. Several Israeli diplomats were invited to the celebration and would arrive on a specially chartered El Al flight. Agents knew Eichmann would have to be smuggled aboard this flight. Harel contacted the members of his select team who had remained in Israel awaiting further orders. Each agent was sent to a different city, from which he would depart for Argentina, supposedly to join the national celebrations. A series of safe houses was established. Once in Argentina, the Mossad agents changed locations and rental cars every day to avoid being tracked. On the evening of May 11, 1960, four agents were positioned in two cars near Eichmann's house on Garibaldi Street. They pretended to have car trouble. Eichmann was late getting home that evening, so two of the agents decided to leave. Two agents remained, continuing to occupy themselves with their car engine. At 8:30 in the evening, Eichmann alighted from his usual bus. He walked over the agents' car, offering assistance. The agents quickly overpowered Eichmann, put him in the car, and drove to the safe house.

The Mossad team had to keep Eichmann in their custody for several days until he could be smuggled aboard the departing El Al flight nine days later. He was shackled to his bed in the safe house, but was cooperative with Mossad agents. The team had counted on Eichmann's family not contacting local police. His family contacted several friends, trying to learn of his whereabouts, but none offered any information. They did not call the police for fear of drawing attention to Eichmann's real identity.

On May 20, 1960, Eichmann was slightly drugged and dressed in the uniform of an El Al crewmember. The agents who accompanied Eichmann were similarly dressed. A few days prior to their departure, the Mossad team sent one of their agents to a local doctor pretending to have a brain injury. He was issued a medical certificate for travel noting possible side effects, such as difficulty walking and speaking. The agents changed the name on the certificate to match Eichmann's new pseudonym, providing an alibi for his behavior while drugged.

Mossad was successful in its long mission. Eichmann landed safely in Israel on May 22, 1960. Eichmann stood trial for war crimes and crimes against humanity in Israel from April 2 to August 14, 1961. He was convicted and sentenced to death.

Eichmann was executed on May 31, 1962.

#### ■ FURTHER READING:

##### BOOKS:

Aharoni, Zvi, Wilhelm Dietl, Meir Amit, and Helmut Bogler (trans.) *Operation Eichmann: The Truth about the Pursuit, Capture and Trial*. New York: John Wiley and Sons, 1997.

Black, Ian and Benny Morris. *Israel's Secret Wars: A History of Israel's Intelligence Services*. New York: Grove Press, 1992.

Isser, Harel. *The House on Garibaldi Street: The First Full Account of the Capture of Adolf Eichmann*. New York: Viking Press, 1975.

##### ELECTRONIC:

The Nizkor Project. <<http://www.nizkor.com>> (November 10, 2002).

##### SEE ALSO

*Gestapo*  
*Mossad*  
*World War II*

---

## Eisenhower Administration (1953–1961), United States National Security Policy

---

■ CARYN E. NEUMANN

To President Dwight D. Eisenhower, the national security of the United States could best be maintained by an interventionist international policy. Under the guidance of Secretary of State John Foster Dulles, his administration abandoned the Cold War policy of containment that had been adopted by President Harry S. Truman in favor of a two-pronged approach to the communist menace. The U.S. would respond militarily to overt communist aggression while advocating active measures to promote the liberation of countries that had converted to communism. This new policy required a strong military and Eisenhower accordingly increased the production of nuclear weapons as a cost-effective way to meet his administration's goals.

Eisenhower won the presidency in 1952 partly because of his record as one of the military heroes of World War II. As president, he sought to maintain America's global presence as the main deterrence to communist expansion, but he regarded military outlays as unproductive. To Eisenhower, every raw material and skill that served the military did so at the expense of the domestic economy. To meet the needs of a steadily growing population, he sought to devote as few resources as possible to the military. This cost cutting led him to emphasize nuclear weapons because they offered more bang for the buck, in both literal and psychological terms.

Popularly thought to have delegated foreign policy strategy to Dulles, Eisenhower in fact controlled its formulation through the mechanism of the National Security Council (NSC). He created the NSC Planning Board to carry out the strategic planning function, while the Operations Coordinating Board coordinated plans for translating approved national strategy into agency operations.

Dulles commanded day-to-day NSC operations and served as foreign policy spokesman for the administration. In time, Dulles became the sole intellectual wellspring of foreign policy conception at the expense of the policy planning staff. The creation of the Southeast Asia Treaty Organization (SEATO) was his effort at reducing communist dangers in the region.

Upon entering office in 1953, Eisenhower immediately had to confront the stalemated Korean War. His administration informed China that further delays in the truce negotiations would enlarge the scale of the war and that a resumption of full-scale fighting might include the American use of nuclear weapons. The Chinese signed an armistice in July 1953. Conflict with China would dominate much of Eisenhower's presidency as the communists periodically tested American intentions before retreating before military threats.

While the Eisenhower administration generally used propaganda and forms of psychological warfare to peacefully weaken communist influence, it occasionally resorted to violence. The pledge to liberate countries from communism meant that limited means would be used to achieve U.S. aims as long as no danger existed of provoking a Soviet-U.S. war. In 1953, the Central Intelligence Agency (CIA) helped stage a coup in oil-rich Iran to replace nationalist and Cold War-neutral Prime Minister Mohammed Mossadegh with the American-allied Shah of Iran. In 1954, the CIA staged another coup to get rid of Guatemalan President Jacobo Arbenz Guzman, a land reformer who had communists among his supporters but lacked any particular ideological ties to the Soviet Union. The involvement of the American government in both operations quickly became widely known.

In order to head off congressional efforts to study the CIA's covert operations following these two coups, Eisenhower commissioned World War II hero Lt. Gen James Doolittle to study the subject. The 1954 Doolittle Report provided an early justification for covert action against communists by stating that no rules applied when faced with an implacable enemy set upon world domination by whatever means and whatever cost. In 1955, the NSC issued NSC-5412/2 to spell out the goals of covert operations. Such activities were to be designed to create and exploit troublesome problems for communism; discredit the prestige and ideology of communism; counter any communist threat to achieve dominant power in a free world country; reduce communist control over any areas of the world; create a positive image of the U.S.; and develop underground resistance to communism.

Eisenhower left office in 1961. His intelligence-related legacy is a mixed one. In 1975, a Senate committee headed by Frank Church charged that the exposure of covert actions in foreign nations damaged the ability of the U.S. to exercise moral and ethical leadership throughout the world. While the Eisenhower administration succeeded in reducing communist influence in the 1950s, the use of

covert operations may have caused damage to the long-term national security interests of the United States.

#### ■ FURTHER READING:

##### BOOKS:

Boll, Michael M. *National Security Planning Roosevelt through Reagan*. Lexington: University Press of Kentucky, 1988.

Crabb, Cecil V. and Kevin V. Mulcahy. *American National Security: A Presidential Perspective*. Pacific Grove, CA: Brooks/Cole, 1991.

Lord, Carnes. *The Presidency and the Management of National Security*. New York: The Free Press, 1988.

##### SEE ALSO

*ADFGX Cipher*

*CIA (United States Central Intelligence Agency)*

*Cold War (1950–1972)*

*Korean War*

*National Security Strategy, United States*

*NSC (National Security Council)*

*NSC (National Security Council), History*

*Nuclear Weapons*

*President of the United States (Executive Command and Control of Intelligence Agencies)*

*Truman Administration (1945–1953), United States National Security Policy*

## Eisenhower Doctrine.

SEE *Cold War (1950–1972)*.

---

## El Salvador, Intelligence and Security

---

El Salvador won its independence from Spain in 1821, and joined the Central American Federation. The nation left the Federation in 1839, establishing its own government. Political rivalry has been endemic in El Salvador, reaching a climax in 1980 when the country erupted in civil war. In 1992, leftist rebel guerrillas and the El Salvadoran government signed a peace treaty. Specified in the agreement were numerous government and military reforms desired by opposition forces. Some of these reforms extended to the El Salvadoran intelligence and security community.

Reforms continue today, but the intelligence community of El Salvador underwent several changes under a program of demilitarization in the 1990s. Secret police and anti-dissident units were abolished, but political espionage remains in practice to a lesser degree.

The main intelligence agency in El Salvador is the *Dirección Nacional Civil* (DNI), National Directorate of Intelligence. The DNI collects and processes both domestic and foreign intelligence information. The agency also coordinates the operations of several smaller intelligence units, including counter-terrorism, counterintelligence, anti-narcotics, and anti-paramilitary forces.

The Ministry of Defense and Public Security manages military intelligence and security forces. Though the army and various militias are responsible for their own strategic intelligence forces, the Ministry of Defense aids in the sharing of information among various agencies, and coordinates large-scale surveillance operations for the C-2, the main military intelligence wing.

The El Salvadoran government also maintains a number of special operations units in the intelligence community. An Anti-Riot Unit (UMO) and the Political Reaction Group (GRP) work with law enforcement to conduct surveillance on anti-government groups and paramilitary organizations. The anti-riot squad has acted as peacekeepers during large protests, and helped stop looting after natural disasters.

As part of its series of reforms, El Salvador legalized the U.S. dollar as official currency, alongside the existing national currency, the colon. The government hopes that the influence of a stronger currency will help the nation recover from the effects of civil war and encourage investment in the region. However, the dual currency also opens the nation to increased financial crimes, including money laundering for drug cartels. Working with neighboring nations, the Organization of American States, and the United Nations, El Salvadoran intelligence forces are acting to combat trafficking and financial crimes related to illegal drugs.

## ■ FURTHER READING:

### ELECTRONIC:

Central Intelligence Agency. "Columbia" CIA World Factbook <<http://www.cia.gov/cia/publications/factbook/geos/es.html>>(April 18, 2003).

## Electroactive Polymers and Devices.

SEE *Biological and Biomimetic Systems*.

## Electromagnetic Pulse

■ LARRY GILMAN

Any nuclear explosion 25 miles (40 km) or higher above the ground produces a high-altitude electromagnetic pulse

(HEMP), a short-lived, overlapping series of intense radio waves that blanket a large swath of ground. These radio waves can induce electrical currents in metallic objects and so cause damage to electrical and electronic equipment, including electrical power grids, telephone networks, radios, and computers. The HEMP produced by a single large (i.e., multi-megaton) nuclear weapon detonated 125 miles (200 km) above the center of the continental United States would affect more than half the country; a weapon detonated at 250 miles (400 km) would affect the entire country, though at lower pulse intensities. Military electronics are often "hardened" against HEMP by enclosures of metal foil and by specialized surge protectors. Civilian systems are not hardened against HEMP.

A typical HEMP consists of a series of overlapping radio pulses, each produced by a different physical aspect of the nuclear explosion. The first, briefest, and most intense component of a HEMP is the prompt gamma signal, which is produced as follows: When a nuclear weapon detonates, large numbers of gamma rays (high-energy photons with wavelengths less than .1 nm) range radiate outward from the burst point. Many of these collide with atoms in the Earth's atmosphere, knocking electrons free. These free electrons are created almost simultaneously in a large volume of the atmosphere surrounding the explosion, and travel rapidly away from the burst point in all directions. Because any charged particle crossing magnetic field lines experiences a force at right angles to its direction of motion, the Earth's magnetic field forces these electrons to follow curved paths, and because charged particles following curved paths emit electromagnetic waves (synchrotron radiation), the explosion-liberated electrons spiraling through the Earth's magnetic field emit a strong radio pulse, namely, the prompt gamma component of the HEMP. Additional pulses, of longer duration but lower magnitude, arrive soon afterward. These are caused by scattered neutrons and gamma rays (radiation that has made one or more bounces, rather than following a straight radial path from the burst point) and by the expansion and ascent of the ionized nuclear fireball through the Earth's magnetic field. The electromagnetic pulse caused by the latter effect, termed the magnetohydrodynamic EMP or HD-EMP, is of low intensity but long duration, and is thought to be a particular threat to power transmission lines.

Although the first nuclear weapon was exploded in 1945, HEMP was unknown to U.S. scientists until July 8, 1962, when a high-altitude nuclear test code-named Starfish was conducted by the U.S. approximately 250 miles (400 km) above the Pacific Ocean, some 800 miles (1280 km) from the Hawaiian island of Oahu. Unexpectedly, some 30 strings of streetlights failed in the island's main town simultaneously with the Starfish explosion. Investigation showed that certain of the lines, randomly oriented so as to pick up the HEMP from Starfish like radio antennae, had absorbed enough energy to blow their fuses. Soviet scientists were probably already aware of HEMP,

because the Soviet Union had already conducted high-altitude tests like Starfish. HEMP subsequently became a central component in strategic nuclear war-simulations; many speculative scenarios for a Soviet first strike on the U.S. began with an EMP “lay-down” created by simultaneously exploding a relatively small number of nuclear weapons at high altitude over the United States. The goal would have been to cause widespread damage to civilian and military electrical and electronics systems at relatively low cost, to be followed by a more devastating ground attack. More recently, some U.S. officials considered a smaller-scale EMP laydown attack on Iraq as a prelude to the Gulf War of 1990. (The attack was not carried out.)

Although some planners have worried that a nation or terrorist group possessing only a few nuclear weapons might use one of them to blanket the U.S. with a damaging HEMP, this is thought by most experts to be unlikely. To create a significant HEMP attack, a weapon must be small enough to be lofted on a ballistic missile, and few countries have the know-how either to make powerful nuclear weapons of such small size or to build ballistic missiles. In any case, it is unlikely that an adversary seeking to cause maximal harm and willing to risk using nuclear weapons against a nuclear-armed adversary such as the U.S. would make a HEMP attack. Any nuclear weapon would cause far more destruction by direct blast (if detonated over or in a city) than by HEMP (if detonated at high altitude).

Besides HEMP, two other forms of electromagnetic pulse may be caused by nuclear explosions. The first is generated inside electronic devices by the passage of ionizing radiation (e.g., neutrons and gamma rays) directly into metallic cases, circuit boards, semiconductor chips, and other components, where it can cause brief electrical currents to flow by knocking electrons loose from atoms. This effect is termed systems-generated electromagnetic pulse (SGEMP). The other form of EMP—source-region EMP or SREMP—occurs when a nuclear weapon explodes at low altitude. In this situation, a highly asymmetric electric field is produced in the vicinity of the burst (e.g., within a radius of 3–8 km) having intensities that are much greater than those produced by HEMP. Since the region affected by SREMP corresponds to that effected by the nuclear blast itself, SREMP is relevant only to the defense of hardened targets such as buried missile silos, which are intended to remain functional even in the aftermath of a near-surface nuclear blast.

Carbon-graphite coils capable of generating an electromagnetic pulse used to destroy electronics equipment—especially communications equipment—can be fitted to cruise missiles. Carbon-graphite equipped cruise missiles were used by U.S.-led forces in raids on Baghdad, Iraq in 1991 and in 2003.

Scientists at Lawrence Livermore National Laboratory reportedly developed an HPM weapon for the Department of Justice: aimed at a moving vehicle, the HPM could shut off the electronic ignition, thus bringing a high-speed car chase to an abrupt end.

## ■ FURTHER READING:

### BOOKS:

“Electromagnetic Pulse Threats to U.S. Military and Civilian Infrastructure.” Hearing Before the Military Research and Development Subcommittee of the Committee on Armed Services, U.S. House of Representatives, Oct. 7, 1999 (H.A.S.C. No. 106–31). Washington, DC: U.S. Government Printing Office, 2000.

### PERIODICALS:

Kruse, V. J., et al. “Impacts of a Nominal Nuclear Electromagnetic Pulse on Electric Power Systems: A Probabilistic Approach.” *IEEE Transactions on Power Delivery*. (Vol. 6, No. 3, July 1991): 1251–1263.

### SEE ALSO

*Nuclear Weapons*

---

## Electromagnetic Spectrum

---

■ LARRY GILMAN

The electromagnetic spectrum consists of all the frequencies at which electromagnetic waves can occur, ordered from zero to infinity. Radio waves, visible light, and x rays are examples of electromagnetic waves at different frequencies. Every part of the electromagnetic spectrum is exploited for some form of military, security, or espionage activity; the entire spectrum is also key to science and industry.

### Basic Physics

Electromagnetic waves have been known since the mid-nineteenth century, when their behavior was first described by the equations of Scottish physicist James Clerk Maxwell (1831–1879). Electromagnetic waves, according to Maxwell’s equations, are generated whenever an electrical charge (e.g., an electron) is accelerated, that is, changes its direction of motion, its speed, or both. An electromagnetic wave is so named because it consists of an electric and a magnetic field propagating together through space. As the electric field varies with time, it renews the magnetic field; as the magnetic field varies, it renews the electric field. The two components of the wave, which always point at right angles both to each other and to their direction of motion, are thus mutually sustaining, and form a wave which moves forward through empty space indefinitely.

The rate at which energy is periodically exchanged between the electric and magnetic components of a given electromagnetic wave is the frequency,  $\nu$ , of that wave and



has units of cycles per second or Hertz (Hz); the linear distance between the wave's peaks is termed its wavelength,  $\lambda$ , and has units of length (e.g., meters). The speed at which a wave travels is the product of its wavelength and its frequency,  $V = \nu\lambda$ ; in the case of electromagnetic waves, Maxwell's equations require that this velocity equal the speed of light,  $c$  (>186,000 miles per second [300,000 km/sec]). Since the velocity of all electromagnetic waves is fixed, the wavelength  $\lambda$  of an electromagnetic wave always determines its frequency  $\nu$ , or vice versa, by the relationship  $c = \nu\lambda$ . The higher the frequency (i.e., the shorter the wavelength) of an electromagnetic wave, the higher in the spectrum it is said to be. Since a wave cannot have a frequency less than zero, the spectrum is bound by zero at its lower end. In theory, it has no upper limit.

**Electromagnetic waves and matter.** All atoms and molecules at temperatures above absolute zero radiate electromagnetic waves at specific frequencies that are determined by the details of their internal structure. In quantum physics, this radiation must often be described as consisting of particles called photons rather than as waves; however, this article will restrict itself to the classical (continuous-wave) treatment of electromagnetic radiation, which is adequate for most technological purposes.

Not only do atoms and molecules radiate electromagnetic waves at certain frequencies, they can absorb them at the same frequencies. All material objects, therefore, are continuously absorbing and radiating electromagnetic waves having various frequencies, thus exchanging energy with other objects, near and far. This makes it possible to observe objects at a distance by detecting the electromagnetic waves that they radiate or reflect, or to affect them in various ways by beaming electromagnetic waves at them. These facts make the manipulation of electromagnetic waves at various frequencies (i.e., from various parts of the electromagnetic spectrum) fundamental to many fields of technology and science, including radio communication, radar, infrared sensing, visible-light imaging, lasers, x rays, astronomy, and more.

## The Spectrum

The spectrum has been divided by physicists into a number of frequency ranges or bands denoted by convenient names. The points at which these bands begin and end do not correspond to shifts in the physics of electromagnetic radiation; rather, they reflect the importance of different frequency ranges for human purposes. Below, the various parts of the spectrum are named in order, lowest-frequency to highest-frequency, and their properties described.

**Radio.** Radio waves are typically produced by time-varying electrical currents in relatively large objects (i.e., at least

centimeters across). This category of electromagnetic waves extends from the lowest-frequency, longest-wavelength electromagnetic waves up into the gigahertz (GHz; billions of cycles per second) range. The U.S. government officially allocates sub-bands of the radio frequency spectrum to various military and commercial purposes from  $9 \times 10^3$  Hz to  $3 \times 10^{11}$  Hz, dividing this part of the spectrum up into over 450 non-overlapping frequency bands. These bands are exploited by different users and technologies: for example, broadcast FM is transmitted using frequencies on the order of  $10^6$  Hz, while television signals are transmitted using frequencies on the order of  $10^8$  Hz (about a hundred times higher). In general, higher-frequency signals can be used to transmit lower-frequency information, but not the reverse; thus a voice signal with a maximum frequency content of 20 kHz (kilohertz, thousands of Hertz) can, if desired, be transmitted on a signal centered in the GHz range, but it is impossible to transmit a television signal over a broadcast FM station. From  $10^9$  to  $3 \times 10^{11}$  Hz, radio waves are termed microwaves; these are used for high-speed communications links, heating food, radar, and electromagnetic weapons, that is, devices designed to irritate or injure people or to disable enemy devices. The microwave frequencies used for communications and radar are subdivided still further into frequency bands with special designations, such as "X band" and "Y band." Microwave radiation from the Big Bang, the cosmic explosion in which the Universe originated, pervades all of space.

**Infrared.** Electromagnetic waves from approximately  $10^{12}$  to  $5 \times 10^{14}$  Hz are termed infrared radiation. The word infrared means "below red," and is assigned to these waves because their frequencies are just below those of red light, the lowest-frequency light visible to human beings. Infrared radiation is typically produced by molecular vibrations and rotations (i.e., heat) and causes or accelerates such motions in the molecules of objects that absorb it; it is, therefore, perceived by the body through the increased warmth of skin exposed to it. Since all objects above absolute zero emit infrared radiation, electronic devices sensitive to infrared can form images even in the absence of visible light. Because of their ability to "see" at night, imaging devices that electronically create visible images from infrared light are important in security systems, on the battlefield, and in observations of the Earth from space for both scientific and military purposes.

**Visible.** Visible light consists of electromagnetic waves with frequencies in the  $4.3 \times 10^{14}$  to  $7.5 \times 10^{14}$  Hz range. Waves in this narrow band are typically produced by rearrangements (orbital shifts) in the outer electrons of atoms. Most of the energy in the sunlight that reaches the Earth's surface consists of electromagnetic waves in this narrow frequency range; our eyes have therefore evolved to be sensitive to this band of the electromagnetic spectrum.

Photovoltaic cells—electronic devices which turn incident electromagnetic radiation into electricity—are also designed to work primarily in this band, and for the same reason. Because half the Earth is liberally illuminated by visible light at all times, this band of the spectrum, though narrow (less than an octave), is essential to thousands of applications, including all forms of natural and many forms of mechanical vision.

**Ultraviolet.** Ultraviolet light consists of electromagnetic waves with frequencies in the  $7.5 \times 10^{14}$  to  $10^{16}$  Hz range. It is typically produced by rearrangements in the outer and intermediate electrons of atoms. Ultraviolet light is invisible, but can cause chemical changes in many substances: for living things, consequences of these chemical changes can include skin burns, blindness, or cancer. Ultraviolet light can also cause some substances to give off visible light (fluoresce), a property useful for mineral detection, art-forgery detection, and other applications. Various industrial processes employ ultraviolet light, including photolithography, in which patterned chemical changes are produced rapidly over an entire film or surface by projecting patterned ultraviolet light onto it. Most ultraviolet light from the sun is absorbed by a thin layer of ozone ( $O_3$ ) in the stratosphere, making the Earth's surface much more hospitable to life than it would be otherwise; some chemicals produced by human industry (e.g., chlorofluorocarbons) destroy ozone, threatening this protective layer.

**X rays.** Electromagnetic waves with frequencies from about  $10^{16}$  to  $10^{19}$  Hz are termed x rays. X rays are typically produced by rearrangements of electrons in the innermost orbitals of atoms. When absorbed, they are capable of ejecting electrons entirely from atoms and thus ionizing them (i.e., causing them to have a net positive electric charge). Ionization is destructive to living tissues because ions may abandon their original molecular bonds and form new ones, altering the structure of a DNA molecule or some other aspect of cell chemistry. However, x rays are useful in medical diagnosis and in security systems (e.g., airline luggage scanners) because they can pass entirely through many solid objects; both traditional contrast images of internal structure (often termed “x rays” for short) and modern computerized axial tomography images, which give much more information, depend on the penetrating power of x rays. X rays are produced in large quantities by nuclear explosions (as are electromagnetic waves at all other frequencies above the radio band), and have been proposed for use in a space-based ballistic-missile defense system as follows: X-rays emitted by an orbital nuclear explosion would stimulate coherent, highly-directional x-ray emission (x-ray lasing) in special fibers placed next to the warhead that had been pre-aimed at ballistic warheads arcing through space. The resulting x-ray laser bursts would disable the warheads or knock them off course. There are, however, many technical and

political problems with such a scheme, and its feasibility has never been demonstrated.

**Gamma rays.** All electromagnetic waves above about  $3 \times 10^{19}$  Hz are termed gamma rays ( $\gamma$  rays). Gamma rays are typically produced by rearrangements of particles in atomic nuclei. A nuclear explosion produces large quantities of gamma radiation, which is both directly and indirectly destructive of life. By interacting with the Earth's magnetic field, gamma rays from a high-altitude nuclear explosion can cause an intense pulse of radio waves termed an electromagnetic pulse (EMP). EMP may be powerful enough to burn out unprotected electronics on the ground over a wide area; most military hardware is therefore “hardened” against EMP to some degree, although hardening standards vary from one sector of the military to another.

**Radio-frequency spectrum allocation.** Radio waves present a unique regulatory problem, for only one broadcaster at a particular frequency can function in a given area. (Signals from overlapping same-frequency broadcasts would be received simultaneously by antennas, interfering with each other.) Throughout the world, therefore, governments regulate the radio portion of the electromagnetic spectrum, a process termed spectrum allocation. In the U.S., since the passage of the Communications Act of 1934, the radio spectrum has been deemed a public resource. Individual private broadcasters are given licenses allowing them to use specific portions of this resource, that is, specific sub-bands of the radio spectrum. The United States Commerce Department's National Telecommunications and Information Administration (NTIA) and FCC (Federal Communications Commission) oversee the spectrum allocation process, which is subject to intense lobbying by various telecommunications stakeholders.

**Military and security significance of the electromagnetic spectrum.** Virtually all forms of military, espionage, and security activity exploit some portion of the electromagnetic spectrum. The transmission, reception, and interception of radio messages are perhaps the most obvious examples, second to the use of light in the visible spectrum for ordinary vision and most technical imaging. More exotic direct applications of electromagnetic radiation are also under development, including the direct use of electromagnetic waves (e.g., laser light) as a destructive weapon, and for various other methods of electronic warfare, defined by the U.S. Joint Chiefs of Staff as “any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy.” Jamming of enemy transmissions and protection of friendly forces against enemy jamming attempts are typical forms of electronic warfare.

In summary, it can be said that the manipulation of every level of the electromagnetic spectrum is of urgent

technological interest, but most work is being done in the radio through the visible portions of the spectrum (below  $7.5 \times 10^{14}$  Hz), where communications, radar, and imaging can be accomplished.

#### ■ FURTHER READING:

##### ELECTRONIC:

"Electromagnetic Spectrum Use in Joint Military Operations." Chairman of the Joint Chiefs of Staff Instruction. May 1, 2000. <[http://www.dtic.mil/doctrine/jel/cjcsd/cjcsi/3320\\_01.pdf](http://www.dtic.mil/doctrine/jel/cjcsd/cjcsi/3320_01.pdf)> (Jan. 30, 2003).

Schroeder, Norbert. "Radio Frequency Spectrum Allocations in the United States." National Telecommunications and Information Administration. July 1, 2000. <[http://www.ntia.doc.gov/osmhome/chart\\_00.htm](http://www.ntia.doc.gov/osmhome/chart_00.htm)> (Jan. 30, 2003).

##### SEE ALSO

*Electromagnetic Weapons, Biochemical Effects*  
*Electronic Countermeasures*  
*Electro-optical Intelligence*

## Electromagnetic Warhead Shrouding.

SEE *Infrared Detection Devices.*

## Electromagnetic Weapons, Biochemical Effects

■ BRIAN HOYLE

Electromagnetic weapons—also known as E-bombs—are designed to release a high-power flash of radio waves or microwaves. Depending on the energy of the electromagnetic pulse, effects can range from the disabling of electronic circuitry to physiological effects in those exposed to the electromagnetic pulse.

The pulse released by an electromagnetic weapon lasts for an extremely short time, around 100 picoseconds (one ten-billionth of a second). The absorption of this blast of high energy by anything capable of conducting electricity, including nerves and neurons, overwhelms the recipient.

Research and development into the effects of electromagnetic weapons on human beings and animals was underway in the 1940s. The Japanese spent considerable sums of money on the development of a "Death Ray" between 1940 and 1945. A review of these studies by the United States military concluded that it was possible to develop a weapon that would produce an electromagnetic

ray capable of killing humans five to 10 miles away from the source.

Animal studies have demonstrated the lethal nature of electromagnetic radiation. In the studies, wavelengths ranging from 60 centimeters destroyed the lung cells of mice and ground hogs. Wavelengths less than two meters also destroyed brain cells.

Electronic stimulation can have other, nonlethal effects on humans. Secret research conducted in the United States following World War II demonstrated that electronic stimulation of different regions of the brain of test subjects could produce extreme emotions of rage, lust, and fatigue. Another research program, dubbed "Operation Knockout," operated at the Allan Memorial Institute in Montreal, Canada, with funding from the Central Intelligence Agency. The study's director, Dr. Ewen Cameron, discovered that electroshock treatments caused amnesia. Memories could be erased, and the subjects reprogrammed. Once these "psychic driving" experiments became public, Cameron—then a pre-eminent psychiatrist, endured harsh public and professional criticism.

In the 1960s, the U.S. Defense Advanced Projects Research Agency (DARPA) studied the health and psychological effects of low energy microwaves for weapons applications. The ability of microwaves to damage the heart, create leaks in blood vessels in the brain, and to produce hallucinations were demonstrated.

Many scientists assume that research into the debilitating effects of electromagnetic radiation has continued up to the present day. However, increasing restrictions on the information obtainable through the U.S. Freedom of Information Act have made verification difficult. A 1993 U.S. Air Command and Staff College paper entitled "Non Lethal Technology and Air Power" documented low frequency, "acoustic" and high power microwave weapons that could deter or debilitate humans.

Low frequency electromagnetic waves, also known as acoustic waves, have been commonly used for decades in functions such as ultrasound machines. However, acoustic waves can also cause internal organs of humans to vibrate. The result can be nausea, diarrhea, earache, and mental confusion. The discomfort increases as one gets closer to the source.

Shorter wavelength electromagnetic radiation produces different effects. A common example is microwave radiation, which in a microwave oven can be used to heat up foods and liquids. When directed at humans, a microwave weapon causes atoms to vibrate, which in turn generates heat. At 200 yards away, body temperature increases from the normal 98.6° F to 107° F. At closer range, the temperature increase can be even higher, and is lethal.

Microwave electromagnetic weapons can also stun a victim. This is the result of the stimulation of peripheral nerves. The simultaneous activity of many nerves overwhelms the capacity of the brain to process the incoming information, and can induce unconsciousness.

The biochemical effect of microwave exposure is dependent on the distance from the source, as electromagnetic fields become much weaker as the distance from the source increases.

Experiments with very low frequency electromagnetic radiation have demonstrated that the radiation can induce the brain to release chemicals that induce slumber, or to release a chemical called histamine. In human volunteers, the histamine release produces flu-like symptoms, which dissipate when the radiation stops.

Not all electromagnetic weapons are cloaked in military secrecy. A device called the Pulse Wave Myotron is commercially available. The Myotron emits rapid pulses of electromagnetic radiation. The pulses incapacitate the movement of voluntary muscles by over riding the electrical pulse that normally flows from nerve to nerve within the muscles. Involuntary muscles, such as the heart and muscles that operate the lungs, are unaffected. Thus, a victim is rendered incapable of movement or speech. The effect lasts until the muscles can repolarize; approximately 30 minutes.

#### ■ FURTHER READING:

##### BOOKS:

Alexander, John B. *Future War: Non-Lethal Weapons in Twenty-First Century Warfare*. New York: St. Martin's Press, 1999.

##### PERIODICALS:

Pasternak, D. "Wonder Weapons." *U.S. News & World Report*. July 7 (1997): 38–46.

##### SEE ALSO

*Electronic Warfare*  
*Energy Directed Weapons*  
*Radio Frequency (RF) Weapons*

---

## Electronic Communication Intercepts, Legal Issues

---

■ MICHAEL J. O'NEAL

The legal issues surrounding the interception of electronic communications are many and varied, primarily because they arise in different contexts: criminal investigations, corporate espionage, employer-employee relationships, and the intelligence activities of the federal government conducted against foreign countries. In recent years, two primary issues have arisen. One, rapid changes in technology can sometimes outpace legislation designed to protect United States citizens from unwarranted electronic

intercepts. Two, in response to the threat of terrorism against the United States, the federal government passed legislation that, in the eyes of some, weakened constitutional protections against unwarranted interception of electronic communications.

**Electronic intelligence.** Traditionally, intelligence-gathering operations have been divided into two broad categories: human and electronic. Human intelligence gathering, or what the intelligence community refers to as HUMINT, involves the use of on-the-scene human operatives who, for example, prepare maps, observe enemy troop movements, steal documents, recruit others to provide information, or physically eavesdrop on conversations.

HUMINT is a dangerous undertaking. The possibility always exists that the operative will be caught, forced to reveal information about his or her activities and purposes, and even imprisoned or executed. For this reason, intelligence agencies whenever possible have come to rely more on electronic intelligence gathering, or ELINT. Spy satellites and high-altitude planes such as the U2, for example, can be used to provide accurate and timely information about troop deployments or missile installations, while wiretaps and hidden microphones allow communications to be intercepted without placing an operative in danger. Further, ELINT can be conducted by those who have no particular training in spycraft (tradecraft) from positions thousands of miles away.

ELINT is divided into two types: trespassory and non-trespassory. As its name suggests, trespassory ELINT requires some sort of trespass; the target's physical premises have to be entered—to install a transmitter or microphone, for example. Non-trespassory ELINT, in contrast, does not require physical invasion of the target premises. Since the end of World War II and throughout the Cold War, the intelligence community has devised various forms of non-trespassory ELINT, enabling it to intercept information transmitted by satellite, radio, cell phone, and microwave transmissions. While ELINT was and is valuable for gathering foreign intelligence, Congress and the public were concerned about possible misuses of it in conducting criminal investigations against U.S. citizens. Accordingly, under Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (the "Wire Tap Statute"), trespassory interception of electronic communications in criminal investigations without a court order was made illegal. In 1986 the Electronic Communications Privacy Act amended Title III to include non-trespassory interception of e-mail, computer communications, and cell phone calls.

**TEMPEST technology.** The chief legal issue surrounding non-trespassory interception of electronic communications stems from the use of the word *communication*. Under the act, it would be illegal for authorities to, for example, tap a phone without a court order, because the purpose of a phone call is to communicate a message. But modern

electronic devices emit all sorts of information that is never intended to be “communicated.” They do so in the form of what are called emanated transient electromagnetic pulses (ETEP), which can be received and reconstructed. A computer screen, for example, displays information in the form of pixels that glow when they are struck by an electron beam. To keep the pixels on a computer screen lit, the electron beam fires perhaps 60 times per second. The beam’s high-voltage electromagnetic emission can be intercepted and read from as far away as a kilometer using classified government technology called TEMPEST, which stands for Transient Electromagnetic Pulse Emanation Standard. Thus, information can be legally intercepted from a computer screen because it is not “communication”; it is merely incidental to the work that the machine is performing.

The potential for abuse is clear. A person or agency with the know-how could intercept from a business computer information that would be beneficial in, for example, making stock market transactions, or steal proprietary information about the development of a new product. But because the U.S. government uses TEMPEST technology to conduct intelligence on foreign governments and potentially to monitor the activities of terrorists, it currently prohibits nongovernment agencies or individuals from owning TEMPEST equipment, making it difficult to research ways to protect legitimate computer users from this modern form of “eavesdropping.”

**Echelon.** In 1947, the United States and Great Britain agreed to join forces to form a “worldwide listening network,” primarily to keep themselves apprised of the activities of the Soviet Union and its allies. In the United States, this agreement in 1971 evolved into Echelon, a global communications interception and surveillance system. In its early days, the U.S.-UK system and Echelon focused on phone and radio traffic. Later, the focus shifted to satellite and microwave communications. More recently, Echelon has also been used to monitor digital communication, principally on the Internet.

The workings of Echelon remain secret; the U.S. government barely acknowledges that it exists, and personnel who work for the agencies of foreign governments with access to Echelon (currently, Australia, Canada, Denmark, Germany, New Zealand, Norway, and Turkey) sign lifetime confidentiality agreements. Echelon functions by tapping numerous sources, including ground-based radio antennae, cable devices, satellites, equipment housed in the U.S. embassies of foreign nations, and the Internet. With regard to the Internet, Echelon can intercept e-mail and file transfers, and by using so-called sniffer devices, it can monitor Web browsing. It then uses a “dictionary” to filter information through key words and addresses, as well as to translate messages and even to interpret their content. It is estimated that Echelon can intercept three *billion* communications per day, including 90 percent of Internet and satellite traffic.

Echelon was formed for the purpose of conducting foreign intelligence operations. Under the Foreign Intelligence Surveillance Act, no proof of criminality has to be shown to conduct such operations; the only safeguard is the secret Foreign Intelligence Surveillance Court, which verifies that the target of an operation is an “agent of a foreign government” rather than a U.S. citizen (or permanent resident alien). Once again, though, the potential for abuse is clear. Many governments have pressured the United States to reveal information on surveillance targets and intelligence operations conducted through Echelon. They are concerned because of reports that economic and business information gathered through Echelon has been passed to American companies, giving them an advantage over their foreign competitors. In recent years, too, civil libertarians have expressed concern that Echelon could be used in a way that violates the Fourth Amendment, which preserves the right of American citizens to be free from unreasonable searches and seizures.

**The USA Patriot Act.** These developments—the pervasiveness of electronic intelligence-gathering capabilities, the existence of sophisticated surveillance technologies, the evolution of Echelon—all coalesced on October 26, 2001, when President George W. Bush signed into law the USA Patriot Act, more formally the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (Public Law 107-56; 115 Stat. 272). The act was passed in response to the terrorist attacks against the United States on September 11 that year. Its goal was to provide law enforcement and the intelligence community with tools to combat international terrorism.

Even before it was signed into law, the bill was controversial. Its supporters argued that it was necessary in an environment when attacks could emanate not only from recognized states with identifiable borders but also from loosely affiliated transnational groups such as militant Islamic extremists. These groups, it was pointed out, include American citizens and others living inside the United States, such as many of the September 11 hijackers. To communicate across national borders, launder money, and channel funds, these groups rely on phones, radio, and especially the Internet, and law enforcement’s efforts to monitor their communications were shackled by legislation that restricted electronic intercepts. The bill’s opponents argued that the act poses significant risk that civil liberties will be infringed and that it does not provide for legislative and judicial overview of the purposes for which such information is used.

The 342-page USA Patriot Act amends fifteen different statutes, including the Electronic Communications Privacy Act, the Computer Abuse and Fraud Act of 1986, and the Foreign Intelligence Surveillance Act. Many of the changes are scheduled to expire on December 31, 2005, unless they are extended by Congress. While many of the changes are minor, they collectively give the Federal Bureau of Investigation (FBI), the Central Intelligence Agency

(CIA), other federal agencies, and local law enforcement sweeping new powers to conduct intelligence operations against terrorists inside the United States. For example, the government can now legally monitor Web surfing, including terms entered into search engines, by informing a judge that doing so could lead to information “relevant” to a terror investigation. Again, civil libertarians fear that a ten-year-old who innocently conducts a Web search for *bomb* or a student doing Internet research on Allah (the name of the deity in the Islamic faith) could actually attract the attention of the CIA—and never know it.

The act made other significant changes in the law. Both the FBI and the CIA had complained that earlier laws requiring a court order to tap a phone were unduly restrictive in the age of cell phones, when a user is not wired to a location and can easily use multiple phones while on the move. Under the USA Patriot Act, they have the authority to conduct roving wiretaps; instead of getting a court order to tap *a phone*, they now can get such an order to tap a person or organization. This means that if a terrorist suspect uses a cell phone, throws it away, then uses another phone, the government can monitor calls made and received on both phones rather than just one. Similarly, the new law makes it easier for the government to get so-called pen/trap orders, referring to “pen register” and “trap-and-trace device” orders. This change authorizes the collection of telephone numbers dialed to and from a particular communication device, including phones of course, but also computers with Internet connections.

Another change involves Internet service providers (ISPs). Previously, the government had to obtain a court order to access the records of an ISP. Now, the government can seek information from ISPs with just a subpoena. This information includes records of session times and durations, network addresses, and methods of payment. The law also authorizes the ISPs themselves to turn over information they believe suggests that a threat against American lives exists. This includes not only “noncontent” information (account numbers, phone numbers, credit card account numbers, and the like) but “content” information—that is, the actual content of messages that suggest a terrorist threat. Again, the purpose of all these changes is to enable law enforcement to monitor the “chatter” of terrorist groups and, on the basis of information gathered, warn the American public about impending threats, thwart terrorist attacks, and round up suspected terrorists.

## ■ FURTHER READING:

### BOOKS:

- Ewing, Alphonse B. *USA Patriot Act*. Hauppauge, N.Y.: Nova Science Publishing, 2003.
- Reams, Bernard D., Jr., and Christopher Anglim, ed. *USA Patriot Act: A Legislative History of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*. Littleton, CO.: Fred B. Rothman, 2002.

Richelson, Jeffrey T. *The Wizards of Langley*. Boulder, CO.: Westview, 2001.

### ELECTRONIC:

- Electronic Frontier Foundation. “EFF Analysis of the Provisions of the USA PATRIOT Act that Relate to Online Activities,” October 31, 2001 <[http://www.eff.org/Privacy/Surveillance/Terrorism/militias/20011031\\_eff\\_usa\\_patriot\\_analysis.html](http://www.eff.org/Privacy/Surveillance/Terrorism/militias/20011031_eff_usa_patriot_analysis.html)>.
- Federation of American Scientists. “Echelon.” <<http://www.fas.org/irp/program/process/echelon.htm>>.
- United Nations. “Echelon: Legal, Political, and Economic Issues of International Surveillance.” <[http://www.unesco.org/webworld/observatory/in\\_focus/290302\\_echelon.html](http://www.unesco.org/webworld/observatory/in_focus/290302_echelon.html)>.

### SEE ALSO

- Bugs (microphones) and Bug Detectors*  
*Bush Administration (2001–), United States National Security Policy*  
*Computer Fraud and Abuse Act of 1986*  
*Computer Hardware Security*  
*Counter-Terrorism Policy, United States*  
*Domestic Intelligence*  
 ECHELON  
*Electromagnetic Pulse*  
*Foreign Intelligence Surveillance Act*  
*Foreign Intelligence Surveillance Court of Review*  
 HUMINT (Human Intelligence)  
*Internet Surveillance*  
*Internet Tracking and Tracing*  
*Patriot Act, United States*  
*Privacy: Legal and Ethical Issues*  
*September 11 Terrorist Attacks on the United States*  
*U-2 Spy Plane*

---

## Electronic Countermeasures

---

Electronic countermeasures (ECM), also known as electronic attack, is a component of electronic warfare (EW), the use or control of electromagnetic energy either in defense, or for the purposes of a military attack on an enemy. Its counterpart is electronic protection or electronic counter-countermeasures (ECCM)—efforts or equipment directed toward the protection of persons or material from the effects of electronic warfare.

Exemplary of electronic countermeasure technology are the systems developed by Bell Helicopter Textron for the U.S. Air Force, tested in the fall of 2002. The CV-22 Osprey tiltrotor, converted from a V-22, was intended for deployment with Air Force Special Operations Command, which has a specialty in low-altitude force insertions under day or night conditions. The aircraft’s suite of integrated radio frequency countermeasures includes technology for threat location and radar jamming. The Air Force subjected the aircraft to three months’ worth of testing suspended in an anechoic chamber, which simulates an ECM environment.



This April 1999 U.S. Air Force file photo shows the F-22 Raptor in a test flight over Edwards Air Force Base in California. The aircraft features multi-spectral countermeasures and wide field-of-regard offensive and defensive sensors. ©AFP/CORBIS.

The U.S. deployment to Iraq in 2003 tested capabilities both in ECM and ECCM. The relative sophistication of Iraqi electronic systems, built by Western-trained engineers and mathematicians, provided a special challenge to planners. Prior to the commencement of the campaign, Army chief of intelligence Lt. Gen. Robert W. Noonan told *Aviation Week & Space Technology* that in the event of war, “one of the first objectives would be to disrupt local fiber-optic networks, and thus, force the Iraqis to rely on less state-of-the-art communication technologies.”

■ FURTHER READING:

BOOKS:

- Chrzanowski, Edward J. *Active Radar Electronic Countermeasures*. Norwood, MA: Artech House, 1990.
- Lothes, Robert N., Michael B. Szymanski, and Richard G. Wiley. *Radar Vulnerability to Jamming*. Boston: Artech House, 1990.

PERIODICALS:

- Phillips, Edward H. “USAF Testing CV-22 Countermeasures.” *Aviation Week & Space Technology* 157, no. 15 (October 7, 2002): 59.

Wall, Robert. “Intelligence Support Seen Crucial to U.N.” *Aviation Week & Space Technology* 157, no. 17 (October 21, 2002): 30.

SEE ALSO

- Electromagnetic Pulse*
- Electromagnetic Spectrum*
- Electronic Warfare*

## Electronic Warfare

Electronic warfare, or EW, is the use or control of electromagnetic energy either in defense, or for the purposes of a military attack on an enemy. There are three components of electronic warfare: electronic countermeasures or electronic attack, electronic counter-countermeasures or electronic protection, and electronic warfare support measures.

**Electromagnetism and the electromagnetic spectrum.** Electromagnetism is the branch of physics devoted to the study



A U.S. Navy EA-6B Prowler carries sophisticated electronic equipment on board for jamming radar. ©REUTERS NEWMEDIA INC./CORBIS.

of electric and magnetic phenomena. Its focus is electromagnetic force, which, along with gravitation and the strong and weak nuclear forces, is one of the four fundamental interactions in nature. Electromagnetic energy is conveyed by means of radiation, which transfers energy without the requirement of a medium such as air or water. Sunlight, which travels to Earth through the vacuum of space, is electromagnetic energy.

Electromagnetic waves travel at the speed of light, and, as their name indicates, involve both electric and magnetic components. If one holds one's right hand, palm perpendicular to the floor and thumb upright, the fingers indicate the direction that an electromagnetic wave is moving; the thumb points in the direction of the electrical field, as does the heel of the hand; and the palm and the back of the hand indicate the direction of the magnetic field, which is perpendicular both to the electrical field and the direction of wave propagation.

The electromagnetic spectrum is the complete range of electromagnetic waves on a continuous distribution from a very low range of frequencies and energy levels,

with a correspondingly long wavelength, to a very high range of frequencies and energy levels, with a correspondingly short wavelength. Included on the electromagnetic spectrum are—in order of energy levels, from lowest to highest—radio waves and microwaves; infrared, visible, and ultraviolet light; x rays, and gamma rays. Although each occupies a definite place on the spectrum, the divisions between them are not firm; as befits the nature of a spectrum, one simply “blurs” into another.

**Using electromagnetic energy in warfare.** The uses of electromagnetism for war are myriad, and range from the application of radar for navigation and locating targets to the use of electronic bombs or “e-bombs” to disrupt an enemy's mechanical and electromagnetic systems. Electromagnetic energy can be used to confuse or deceive an enemy, as for instance in radar-jamming applications or the propagation of misleading signals. It can also be used directly as a weapon to disable infrastructure.

The three principal components of electronic warfare are:



1. Electronic attack or electronic countermeasures: The use of electromagnetic or directed energy against personnel or equipment with the aim of degrading or destroying combat capabilities.

2. Electronic protection or electronic countermeasures: Efforts or equipment directed toward the protection of persons or material from the effects of electronic warfare. These includes the unintended side-effects of friendly electronic warfare, as well as enemy actions undertaken for the purpose of degrading or destroying one's combat capabilities.

3. Electronic warfare support: Actions and resources committed toward locating, identifying, and if necessary intercepting or neutralizing sources of electromagnetic energy that pose an immediate threat.

#### ■ FURTHER READING:

##### BOOKS:

Browne, J. P. R. *Electronic Warfare*. London: Brassey's, 1998.

Hoffman, Lance J. *Rogue Programs: Viruses, Worms, and Trojan Horses*. New York: Van Nostrand Reinhold, 1990.

Price, Alfred. *War in the Fourth Dimension: U.S. Electronic Warfare, from the Vietnam War to the Present*. London: Greenhill, 2001.

Schleher, D. Curtis. *Electronic Warfare in the Information Age*. Boston: Artech House, 1999.

##### PERIODICALS:

Wall, Robert. "Focus on Iraq Shapes Electronic, Info Warfare." *Aviation Week & Space Technology*. 157, no. 19 (November 4, 2002): 34–35.

———. "Military Launches New EW Efforts." *Aviation Week & Space Technology*. 157, no. 19 (November 4, 2002): 35–43.

##### SEE ALSO

*Electromagnetic Pulse*  
*Microwave Weaponry, High Power (HPM)*

## Electro-Optical Intelligence

Electro-optical "intelligence" involves the acquisition of data from the portion of the electromagnetic spectrum of wavelengths that contains ultraviolet radiation, visible light, and infrared radiation.

The term intelligence refers to the use to which the optical spectrum is put. Ultraviolet, visible, and infrared rays can be collected and analyzed for the information they contain. For example, the detection of infrared radiation—either via satellite or localized detection devices—can reveal the location and movements of humans and heat-generating machinery.

Other analyses can reveal information about the composition of the object that is emitting the radiation. For example, the exhaust of a missile can be detected and distinguished from the exhaust of a commercial aircraft.

Electro-optical analysis equipment most commonly includes forms of radiometers, spectrometers, lasers, and laser radar devices.

Radiometers such as the Advanced Very High Resolution Radiometer operated by the National Oceanographic and Atmospheric Administration, and the Multi-angle Imaging SpectroRadiometer operated by the National Aeronautics and Space Administration provide detailed views of the Earth's surface. For example, the removal of vegetation from an area due to clearing and/or construction is readily detected. While used predominantly for climate studies, these instruments may also provide detailed views that allow critical assessment of the industrial and/or military development in a surveyed area.

A laser radar sends out pulses of a laser beam. The beam, a constrained and narrow beam of light, will ultimately encounter an object and be reflected, still as a tightly organized beam. When the beam returns to the source, a detector can measure the time taken for the beam to travel to the object and return. The distance from the source to the object can be measured very accurately over extremely long distances (i.e., Earth to the Moon).

The United States Army's Pulsed Laser Vulnerability Test System (PLVTS) is a CO<sub>2</sub> laser that can be housed in a portable vehicle. The unit can be taken to whatever test or military site requires accurate radar measurements. The PLVTS has been used in the evaluation of the M-1 tank, Black Hawk helicopter, and various missile test launches.

Another aspect of electro-optical intelligence involves the use of cameras that can record information in both the visible and infrared spectra. Because the infrared emissions from objects occur at night as well as during the day, these cameras are capable of gathering information both in day time and at night. Such cameras have been used in high altitude "spy planes" and other reconnaissance aircraft to develop intelligence concerning ground operations shrouded by clouds associated with weather fronts or more permanently obscured by thick indigenous fog or pollution.

Similarly, visible and infrared imaging is incorporated into telescopes operated by the U.S. Space Command in Haleakala, Maui (TEAL BLUE) and Malabar, Florida (TEAL AMBER). The telescopes are used for the tracking of satellites orbiting the Earth (including reconnaissance satellites) and those that are deeper in space.

#### ■ FURTHER READING:

##### BOOKS:

Gaffney, Timothy, R. *Secret Spy Satellites: America's Eyes in Space*. Berkeley Heights, NJ: Enslow Publishers Inc., 2000.

Kupperberg, Paul. *Spy Satellites (The Library of Satellites)*. New York: Rosen Publishing Group, 2003.

#### ELECTRONIC:

Institute for Defense Studies and Analysis. "Shaping the Land Battle through Remote Sensing and Satellite-Imagery." JNU Campus. February, 2000. <<http://www.idsa.org/an-feb00-5.html>>(26 December 2002).

#### SEE ALSO

*Electromagnetic Spectrum*  
*Electronic Warfare*  
*EM Wave Scanners*  
*Infrared Detection Devices*  
*Laser Listening Devices*  
*Lasers*  
*LIDAR (Light Detection and Ranging)*  
*Microscopes*  
*Satellites, Non-Governmental High Resolution*  
*Satellites, Spy*  
*Spectroscopy*

---

## Electrophoresis

---

Diseases caused by microorganisms are a threat to national security. Even in countries with well-developed healthcare systems, a massive outbreak can strain healthcare infrastructure. In other countries that are less wealthy and more politically volatile, the ravages of disease can sow the seeds of resentment against the more wealthy countries of the West. Thus, it is in a country's best interests to combat infectious diseases. One strategy is to examine the relevant microorganisms, particularly to find out the component(s) that are responsible for the infection. For many microbes, proteins are an important factor in the development of a disease. Proteins can function as receptors, to allow the microorganism to adhere to the surface of a host cell. As well, the toxins produced by microbes such as *Escherichia coli* O157:H7 and *Vibrio cholerae* are proteins. Methods that can "dissect" microorganisms into their components, and which can compare a non-disease causing strain of a microbe to a disease-causing strain to see what their differences are, is a valuable approach to fighting infectious disease. Electrophoresis is especially well suited to this role. Furthermore, specialized types of electrophoresis (i.e., pulsed field electrophoresis) allow the genetic material of the microorganism to be examined. Thus, electrophoresis can reveal much detail at the molecular level.

Electrophoresis is a sensitive analytical form of chromatography. Under the influence of an electrical field charged molecules can be separated from one another as they pass through a gel. The degree of separation and rate of molecular migration of mixtures of molecules depends

upon a variety of factors, which can be tailored depending upon the intent of the separation. For example, conditions can be established that allow molecules of very large mass, but which differ from each other by only a fraction, to be visually separated. The factors that influence molecular separation include the individual size and shape of the molecules, their molecular charge, strength of the electric field, the type of support medium used (e.g., gels made of cellulose acetate, starch, paper, agarose, polyacrylamide) and the conditions of the medium (e.g., ion strength and concentration, pH, viscosity, temperature).

The advent of electrophoresis revolutionized the methods of protein analysis. Swedish biochemist Arne Tiselius was awarded the 1948 Nobel Prize in chemistry for his pioneering research in electrophoretic analysis. Tiselius studied the separation of serum proteins in a tube (subsequently named a Tiselius tube) that contained a solution subjected to an electric field.

In electrophoresis, the electric charge often is passed through what is known as a support medium. As summarized above, various support media can be used. They all share the trait that they are a three-dimensional arrangement of intertwined strands, which produces holes (or pores) through the gel matrix. Such matrices act as a physical sieve for macromolecules.

In general, the medium is mixed with a chemical mixture called a buffer. The buffer carries the electric charge that is applied to the system. The medium/buffer matrix is placed in a tray. Samples of molecules to be separated are loaded into wells or slots that have been formed at one end of the matrix. As electrical current is applied to the tray, the matrix takes on this charge and develops positively and negatively charged ends. As a result, molecules that are negatively charged such as deoxyribonucleic acid (DNA), ribonucleic acid (RNA), and protein are pulled toward the positive end of the gel.

Because molecules have differing shapes, sizes and charges they are pulled through the matrix at different rates and this, in turn, causes a separation of the molecules. Generally, the smaller and more charged a molecule, the faster the molecule moves through the matrix.

Intact DNA is so large that it cannot move through the pores of a gel (although the technique of pulsed field electrophoresis does allow very large pieces of DNA to be examined). When DNA is subjected to electrophoresis, the DNA is first cut into smaller pieces by restriction enzymes. Restriction enzymes recognize specific sequences of the building blocks of the DNA and cut the DNA at the particular site. There are many types of restriction enzymes, and so DNA can be cut into many different patterns. After electrophoresis, the pieces of DNA appear as bands (composed of similar length DNA molecules) in the electrophoresis matrix.

Proteins have net charges determined by charged groups of the amino acids from which they are constructed. Proteins can also be amphoteric compounds (a

compound that can take on a negative or positive charge depending on the surrounding conditions.) A protein in one solution might carry a positive charge in a particular medium and thus migrate toward the negative end of the matrix. In another solution the same protein might carry a negative charge and migrate toward the positive end of the matrix. For each protein there is a pH in which the protein molecule has no net charge (the isoelectric point). By varying the pH in the matrix, additional refinements in separation are possible.

Sodium dodecyl sulfate (SDS) polyacrylamide gel electrophoresis techniques pioneered in the 1960s provided a powerful means of protein separation. Still, because proteins of similar mass did not always clearly separate into discrete bands in the gel only small numbers of molecules could be separated.

The development in the 1970s of a two-dimensional electrophoresis technique allowed greater numbers of molecules to be separated. Two-dimensional electrophoresis is actually the fusion of two separate separation procedures. The first separation (dimension) is achieved by isoelectric focusing (IEF) that separates protein polypeptide chains according to the arrangement of amino acids that comprise a chain. IEF is based on the fact that proteins will, when subjected to a pH gradient, move to their isoelectric point. The second separation is achieved via SDS slab gel electrophoresis, which separates the molecule by molecular size. Instead of broad, overlapping bands, the result of this two-step process is the formation of a two-dimensional pattern of spots, each comprised of a unique protein or protein fragment. These spots are subsequently subjected to staining and further analysis.

Electrophoresis can be combined with the prior addition of a radioactive food source to the culture of bacteria. The bacteria will use the food to make new proteins, which will be radioactive. Following electrophoresis, the gel can be placed in contact with x-ray film. The radioactive bands or spots will register on the film, and so will determine what proteins were being made at the time of the experiment.

There are many other variations on gel electrophoresis with wide-ranging applications. These specialized techniques include Southern, Northern, and Western Blotting. Blots are named according to the molecule under study. In Southern blots, DNA is cut with restriction enzymes then probed with radioactive DNA. In Northern blotting, RNA is probed with radioactive DNA or RNA. Western blots target proteins with radioactive or enzymatically-tagged antibodies.

Modern electrophoresis techniques now allow the identification of DNA sequences that are the same, and have become an integral part of research into gene structure, gene expression, and the diagnosis of heritable diseases. Electrophoretic analysis also allows the identification of bacterial and viral strains and is finding increasing acceptance as a powerful forensic tool.

## ■ FURTHER READING:

### BOOKS:

- Birren, Bruce W., and Eric Hon Cheong Lai. *Pulsed Field Electrophoresis: A Practical Guide*. San Diego: Academic Press, 1997.
- Rabilloud, Thierry. *Proteome Research: Two-Dimensional Gel Electrophoresis and Identification Methods (Principles and Practice)*. Berlin: Springer Verlag, 2000.
- Westermeier, Reiner. *Electrophoresis in Practice*. Weinheim: Vch Verlagsgesellschaft 2001.

### ELECTRONIC:

- Colorado State University. "Gel Electrophoresis of DNA and RNA." Biomedical Hypertextbooks. January 15, 2000. <<http://arbl.cvmbs.colostate.edu/hbooks/genetics/biotech/gels/>>(5 January 2003).

### SEE ALSO

- Chemical and Biological Detection Technologies*  
*DNA Recognition Instruments*  
*Microbiology: Applications to Espionage, Intelligence and Security*  
*Thin Layer Chromatography*

## ELINT (Electronics Intelligence).

SEE *SIGINT (Signals Intelligence)*.

---

## EM Wave Scanners

---

In order to observe phenomena that cannot be glimpsed through direct contact, for example, the activities of an isolated weapons-testing site in a hostile nation, it may be necessary to employ remote-sensing equipment and techniques. These typically involve views from the air or from space, which require the use of electromagnetic radiation (EMR) across a wide spectrum. Though the information rewards can be high, intelligence services using electromagnetic (EM) scanners in space must deal with a variety of challenges in data collection and analysis.

**Electromagnetic radiation from the sun.** Light from the sun is electromagnetic radiation, and it contains both electric and magnetic components. The direction of propagation for an electromagnetic wave is mutually perpendicular with directions of its electrical and magnetic fields, whereas the electrical field might be thought of as the x-axis on a Cartesian coordinate plane, and the magnetic field the y-axis, the direction of wave propagation is the z-axis.

About 30% of the electromagnetic radiation from the sun that reaches Earth is reflected back into space unchanged, without entering Earth's atmosphere. This is due

to the planet's albedo—its reflective power, or the proportion of incoming radiation that it reflects. Another 25% of solar radiation is absorbed by the atmosphere, while about 45% is absorbed at the planetary surface by living and non-living materials. This energy is later re-radiated to space in degraded form, that is, at a longer wavelength.

The atmosphere and its current conditions have a powerful effect on the amount of visible light reflected, and this—along with the loss of electromagnetic energy from the sun—places constraints on the observational abilities of remote-sensing equipment.

**Detecting images.** There is a continuous distribution of electromagnetic energy levels, from extremely low to extremely high, that together constitutes the entire electromagnetic spectrum of energy. At the lowest level are radio waves, then microwaves (the section of the spectrum across which television transmission takes place). Higher in frequency and energy levels are such forms of light as infrared, visible, and ultraviolet. Still higher are x rays, and highest of all are gamma rays, which have an extremely small wavelength and extremely high frequency.

Of most interest in remote sensing are the energy levels near the middle of the spectrum: microwaves, infrared, visible light, and ultraviolet light. Remote sensing satellites measure the EMR reflected from features on Earth back into space. Photographic cameras on remote-sensing satellites are capable of detecting light from the near infrared to the near ultraviolet. Remote sensing equipment typically divides the infrared portion into relatively low-energy near-infrared images, and higher energy thermal infrared images. The satellite may have a thermal scanner that operates in the thermal infrared portion, or a multi-spectral scanner operating across a range from ultraviolet to thermal infrared. There may also be passive microwave and active radar systems operating in the microwave portion of the spectrum.

**Scanning and processing images.** Satellites equipped with multi-spectral scanners can make precise measurements across a number of narrow bands. These scanners may be of the oscillating or “wisk-broom” type, which scan along a line perpendicular to that of the satellite's trajectory, or of the “push-broom” type, which detect entire scan lines at once.

These multi-spectral scanners record electromagnetic radiation as electrical signals, convert them to digital format, and transmit the information to an Earth receiving station. The latter interprets various numbers as brightness values on a gray scale. Depending on the needs of the observing agency, images may be adjusted for resolution. For example, spatial resolution improves the detail for smaller objects, while radiometric resolution allows for the greatest levels of contrast. The analyzing agency may, in the digital image processing phase, add false color to enhance the readability of images for specific data—for

example, red to indicate heat levels at areas where weapons are being tested.

## ■ FURTHER READING:

### BOOKS:

- Chen, C. H. *Information Processing for Remote Sensing*. River Edge, NJ: World Scientific, 1999.
- Dehqanzada, Yahya A., and Ann Florini. *Secrets for Sale: How Commercial Satellite Imagery Will Change the World*. Washington, D.C.: Carnegie Endowment for International Peace, 2000.
- Firschein, Oscar, and Thomas M. Strat. *RADIUS: Image Understanding for Imagery Intelligence*. San Francisco, CA: Morgan Kaufmann Publishers, 1997.
- Krepon, Michael. *Commercial Observation Satellites and International Security*. New York: St. Martin's Press, 1990.

### ELECTRONIC:

- “Earthshots: Satellite Images of Environmental Change (U.S. Geological Survey).” <<http://edcwww.cr.usgs.gov/earthshots/slow/tableofcontents>> (February 26, 2003).
- “Remote Sensing Data and Information.” <<http://rsd.gsfc.nasa.gov/rsd/RemoteSensing.html>> (February 26, 2003).
- “Satellite Remote Sensing.” University of Waterloo Faculty of Environmental Sciences. <<http://www.fes.uwaterloo.ca/crs/geog165/srs.htm>> (February 26, 2003).
- “Visualization of Remote Sensing Data.” <<http://rsd.gsfc.nasa.gov/rsd/>> (February 26, 2003).

### SEE ALSO

*Satellites, Spy*

## Emergency Response Teams

Emergency response teams are the front line of the Environmental Protection Agency (EPA) Emergency Response Program, which is in turn at the center of the national infrastructure for responding to environmental hazards such as oil spills. The Emergency Response Program brings together a wide range of activities directed toward ensuring appropriate, timely responses in the event of an emergency involving the release of oil or hazardous substances. After state and local first-responder capabilities have been exceeded, emergency response teams provide additional support to see that all hazards are dealt with in accordance with federal guidelines for the safety of human populations and the natural environment.

**The larger framework.** The EPA response system is part of a larger national framework designed to respond to hazards such as the release of toxic chemicals and oil. Among the key facilities is the National Response Center operated by the Coast Guard, which is the first point of contact for



An emergency response team heads to the site of a mock biological threat during a bioterrorism training exercise at Camp Blanding, Florida in 2002. AP/WIDE WORLD PHOTOS.

reporting environmental hazards and other related public emergencies. Linked to the Response Center is the National Response Team, an interagency group co-chaired by EPA and the Coast Guard.

Just as there is a national infrastructure for hazard response, with EPA as a key component, there are guidelines governing the response at the state and local level. This is especially important because in a real-world situation, the personnel most readily available to assist on the scene will likely be local authorities and not functionaries dispatched by Washington.

Local community responses to environmental hazards are guided by the Emergency Planning and Community Right-to-Know Act or EPCRA, passed by Congress in 1986. EPA plays a key role in administering EPCRA, which groups federal agencies into 12 functional areas (for example, Hazardous Substances, which includes EPA) for emergency support.

**The National Response System.** Each year within the United States, there are some 20,000 emergencies that involve the release, or the potential release, of oil, toxins, and other hazardous substances. While local firefighters, emergency personnel, and police occupy the most visible role in responding to these emergencies, they are supported

behind the scenes by the National Response System, in which EPA again is a key player.

The National Response System is designed to act quickly and effectively in emergencies involving oil and hazardous substances. A multi-tiered network, it involves representatives of not only local, state, and federal governments, but also industry and other groups whose knowledge and equipment are necessary to address a chemical threats to human safety and the environment.

**The National Contingency Plan.** Guiding the National Response System is the National Contingency Plan (NCP), also known as the National Oil and Hazardous Substances Pollution Contingency Plan. Described by EPA as a federal blueprint for emergency responses, the NCP evolved over the final third of the twentieth century, as the leadership of the United States and the industrialized world became increasingly aware of the threat that oil spills and accidental releases of chemicals could pose to societies.

A 1967 oil spill caused by the sinking of the tanker *Torrey Canyon*, which dumped more than 37 million gallons of crude oil off the British coast, prompted the development of the first NCP in the following year. Observing the massive damage with which their British counterparts were faced, U.S. officials sought to achieve a system for reporting of accidents, containment of spills, and cleanup of affected sites. The system was designed to include a response headquarters, a national reaction team, and regional teams. These teams were the forerunners, respectively, of the national and regional response teams.

The congressional passage of the Clean Water Act in 1972 led to the revision of the NCP in 1973 to incorporate a plan for the response not only to oil spills, but also to hazardous substance spills. In 1980, Congress passed the Superfund legislation, or the Comprehensive Environmental Response, Compensation, and Liability Act. As a result, the scope of the NCP grew to include the release of substances at hazardous waste sites where emergency removal actions are required. Passage of the Oil Pollution Act of 1990 prompted more changes to the NCP in 1994.

**The Emergency Response Program.** The principal aims of the Emergency Response Program are to take necessary steps toward the prevention of oil spill and hazardous substance emergencies; to prepare local, state, and federal emergency response personnel to deal with such situations; and to respond in a timely and effective manner to incidents as those arise.

The Emergency Response program involves coordination of the ten superfund regions into which the nation is divided geographically, and of five EPA organizations. The latter include the Office of Emergency and Remedial Response, which directs domestic emergency responses; the Chemical Emergency Prevention and Preparedness Office, which oversees responses to chemical emergencies; the Prevention, Pesticides, and Toxic Substances

program, which mobilizes community resources; the Radiation program; and the Office of Underground Storage Tanks, which protects against the release of petroleum from underground tanks.

An example of the EPA emergency response teams at work alongside their counterparts from other federal agencies occurred in the aftermath of the September 11, 2001, terrorist attacks, when the EPA sent more than 200 personnel to the World Trade Center and Pentagon sites. Among their ranks were specialists whose roles are not commonly associated with EPA in the public imagination, including criminal investigators, forensic scientists, and technical experts.

#### ■ FURTHER READING:

##### BOOKS:

*An Overview of the Emergency Response Program.* Washington, D.C.: U.S. Environmental Protection Agency, 1992.

##### PERIODICALS:

Hogue, Cheryl. "Regulators at Scenes of Attacks." *Chemical & Engineering News* 79, no. 39 (September 24, 2001): 11.

Wallgren, Christine. "EPA Team Does Its Work Behind the Scenes." *Boston Globe*. (August 1, 2002): 1.

##### ELECTRONIC:

Emergency Response Program. U.S. Environmental Protection Agency. <<http://www.epa.gov/superfund/programs/er/>> (February 23, 2003).

U.S. National Response Team. <<http://www.nrt.org/production/nrt/home.nsf>> (January 22, 2003).

##### SEE ALSO

*Chemical Safety: Emergency Responses*  
*Coast Guard National Response Center*  
*EPA (Environmental Protection Agency)*  
*National Response Team, United States*

---

## Encryption of Data

---

#### ■ LARRY GILMAN

Data are any useful information and encryption is any form of coding, ciphering, or secret writing. Encryption of data, therefore, includes any and all attempts to conceal, scramble, encode, or encipher any information. In the modern world, however, the term data usually implies digital data, that is, information in the form of binary digits ("bits," most often symbolized as 1s and 0s). Digital data are stored, transferred, and processed in increasingly large quantities at virtually every level of government and in the private sector, especially in industrialized countries. Money is transferred between accounts or disbursed from

automatic teller machines on the basis of exchanges of digital data; medical records, criminal records, tax records, personal documents and telephone conversations, business negotiations, diplomatic communications, and military communications are all, almost without exception, cast into digital form before being transmitted or stored. All transmission media are vulnerable, however, to interception, and stored records may be accessed by unauthorized persons. The need for encryption of digital data is almost universal; anyone who transfers or stores important digital data has an interest in its security.

Governments have always had the strongest interest in data encryption, both as users of ciphering and coding systems (cryptosystems) and as attackers of the cryptosystems of other governments. The United States government, for example, uses encryption for transmission not only of classified (officially secret) data, but also of many unclassified data. Encryption is thus, distinct from classification. Classification is the official assignment of a particular degree of secrecy to data, whereas encryption refers to the translation of data, classified or not, into a form that is difficult for unauthorized parties to read.

**Methods of encryption.** Because digital data are numerical, their efficient encryption demands the use of ciphering rather than coding. A cipher is a system of rules for transforming any message text (the plaintext) into an apparently random text (the ciphertext) and back again. Digital computers are ideal for implementing ciphers; virtually all ciphering today is performed on digital data by digital computers.

The U.S. military, the State Department, and the intelligence agencies (including the Central Intelligence Agency, Federal Bureau of Investigation, National Security Agency [NSA], and others), utilize a variety of secret ciphering methods or "cryptosystems," whose nature is classified and about which little information is publicly available. The NSA, which is dedicated to eavesdropping—that is, to the collection of "signals intelligence" (sigint) both in the U.S. and globally, devotes millions of dollars annually to the breaking of ciphers and codes, and is the world's leading employer of mathematicians and purchaser of computer hardware. In the military, different cryptosystems are employed to achieve different levels of security, ranging from person-to-person communications on the battlefield to the exchange of messages with nuclear submarines at sea and other critical, high-end applications where budgets run high.

Government departments handling nonclassified information, industrial and academic organizations, and private individuals produce and transmit even greater quantities of data than do the military, intelligence agencies, and other handlers of classified data. Because of both the private sector and governmental need for reliable, standardized ciphering of nonclassified data, the National Bureau of Standards (an arm of the federal government) first solicited proposals for "cryptographic algorithms for

protection of computer data during transmission and dormant storage" in 1973 (*Federal Register* 38, No. 93, May 15, 1973). An algorithm developed by German-American cryptographer Horst Feistel, then working for IBM, was eventually chosen as the federal Data Encryption Standard (DES) on July 15, 1977. All information about the DES cipher algorithm is public and no licensing fees need be paid by anyone who wishes to incorporate it into a product. Thus, from 1977 to the present, DES has been built into thousands of data products, becoming among the most widely used cipher in history.

DES is a block cipher, meaning that it chops the message bitstream into blocks or sequences of 64 bits each, then produces a 64-bit ciphertext block by processing the message block through an algorithm (series of mathematical operations) governed by a key (secret number, in this case a 56-bit binary number). The ciphertext block appears to be a random string of bits; to recover the original message block, the 56-bit key that was used to encipher it must be given, stolen, or guessed.

When first implemented, DES was effectively unbreakable—except, probably, by the NSA, which reportedly lobbied the National Bureau of Standards to keep the key length down to a level that NSA supercomputers could cope with. Key length is a basic aspect of cipher security because any cipher can in theory be cracked by the brute-force method known as exhaustion, that is, the trying out of every possible key. In the case of DES, there are  $2^{56} > 72,000,000,000,000,000$  ( $72 \times 10^{16}$ ) possible keys. For many years, DES-enciphered data were safe because few organizations possessed the computing power to test  $72 \times 10^{16}$  keys in a reasonable time, but this ceased to be true several years ago. In July, 1998, a team of cryptographers cracked a DES-enciphered message in 3 days by the exhaustion method, and in 1999 a network of 10,000 desktop PCs cracked a DES-enciphered message in less than a day. DES was clearly no longer invulnerable, but a replacement was not yet in view; users therefore switched to an algorithm termed "triple DES." Triple DES encrypts a plaintext block using one 56-bit key, re-encrypts the resulting ciphertext block using a second 56-bit key, and then re-encrypts the result of the second encryption using a third 56-bit key. However, cryptographers have determined that triple DES is unsatisfactory as a long-term solution, and in 1997, the National Institute of Standards and Technology (NIST) solicited proposals for a cipher to replace DES entirely, the Advanced Encryption Standard (AES).

An algorithm named Rijndael (pronounced RAIN doll), created by Belgian cryptographers Vincent Rijmen and Joan Daemen, was announced as the AES in December, 2001 (Federal Information Processing Standard 197). AES is structurally similar to DES—both are block ciphers, for example—but AES uses blocks and keys that are 128, 192, or 256 bits long (at the user's discretion—longer blocks and keys entail slower processing), rather than a mere 56 bits long as in the original DES. According to the NIST, a computer that could try out all possible 56-bit DES keys in

one second would require approximately  $1.49 \times 10^{14}$  years to try out all possible 128-bit AES keys. Triple DES is still the most commonly-used cryptosystem for the encryption of data and will remain an approved cryptographic standard for the foreseeable future; however, AES has started appearing in commercial products.

Encryption scientists expect that AES will remain secure for at least twenty years. However, in September 2002, two cryptographers—Nicolas Courtois of France, and Josef Pieprzyk of Australia—announced that they had designed an attack on AES that would reduce the number of calculations to crack the cipher from order  $2^{256}$  (for the longest key option) to order  $2^{100}$ . This remains beyond the capabilities of present-day computers, but raises concern for the long-term security of AES.

Both DES and AES are symmetrical-key cryptosystems, meaning that both the sender and receiver must be in possession of an identical secret key to encrypt and decrypt messages to each other. Systems based on public-key cryptography have also become important in the last decade or so, especially the RSA system (named for its inventors, Ronald Rivest, Adi Shamir, and Leonard Adleman). Public-key systems are widely favored for occasional transmissions among networks of users, rather than for dedicated links. RSA has been licensed to the makers of Web browsers such as Netscape and Explorer, allowing their users to employ public-key cryptography for sending encrypted e-mails, making online purchases, and doing online banking (most often without knowing that they are employing cryptography at all). RSA has also been used, without authorization, in the freeware program known as PGP (pretty good privacy). PGP can be downloaded for free from a number of Web sites for personal use.

#### ■ FURTHER READING:

##### BOOKS:

Meyer, Carl H., and Stephen M. Matyas, *Cryptography: A New Dimension in Computer Data Security*. New York: John Wiley & Sons, 1982.

Singh, Simon. *The Code Book*. New York: Doubleday, 1999.

##### PERIODICALS:

"Race to Pick a Better Cipher." *Science* no. 5382 (1998): 1411.

Seife, Charles. "Crucial Cipher Flawed, Cryptographers Claim." *Science* no. 5590 (2002): 2193.

##### ELECTRONIC:

National Institute of Standards and Technology. "Advanced Encryption Standard: Questions and Answers." Computer Resource Security Center. March 5, 2001. <<http://csrc.nist.gov/encryption/aes/round2/aesfact.html>> (November 16, 2002).

Nechvatal, James, et al. "Report on the Development of the Advanced Encryption Standard." National Institute of Standards and Technology. October 2, 2000.

<[csrc.nist.gov/encryption/aes/round2/r2report.pdf](http://csrc.nist.gov/encryption/aes/round2/r2report.pdf)> (Nov. 16, 2002).

## SEE ALSO

*Codes and Ciphers*

# Enduring Freedom, Operation

■ JUDSON KNIGHT

Operation Enduring Freedom was the initial United States military response to the attacks of September 11, 2001, in which almost 3,000 Americans and other nationalities were killed by members of the al-Qaeda terror network. When the Taliban, Islamist extremists who controlled Afghanistan, refused to surrender al-Qaeda leader Osama bin Laden, the United States launched its attack the following month on October 7. The operation, initially named “Infinite Justice,” was accompanied by a homeland security military effort named Noble Freedom. A part of Enduring Freedom was Operation Anaconda, an undertaking to root out al-Qaeda and Taliban personnel in northern Afghanistan. With the success of Enduring Freedom in 2002, the United States would go on a year later to the second phase of its war on terrorism: Operation Iraqi Freedom.

## Stages of the Conflict

After the bombing of two U.S. embassies in Africa in 1998, the administration of President William J. Clinton conducted retaliatory air strikes on a terrorist training camp in Afghanistan, where bin Laden was believed to be in hiding. The air strikes failed to neutralize al-Qaeda, however, and after September 11, President George W. Bush demanded that the Taliban turn bin Laden over to the United States.

The Taliban stalled for weeks, claiming no knowledge as to bin Laden’s whereabouts, while the Bush administration prepared for war. Rather than undergo a lengthy process of obtaining United Nations approval for a multinational force, Bush called on the help of America’s major ally among the major world powers: the United Kingdom. (Canada and Australia later also contributed troops to the coalition force.) On October 7, U.S. and British forces launched air strikes against Afghanistan.

On October 25, approximately 25 aircraft (including 15 carrier-based tactical planes and eight to 10 long-range bombers) struck seven strategic targets, including military training facilities, surface-to-air missile storage sites, and al-Qaeda infrastructure. By November 9, the northern city of Mazar-e-Sharif had fallen to the Northern Alliance, a loose coalition of Afghan factions opposed to the Taliban.

Four days later, a combination of allied air assaults and ground maneuvers by the Northern Alliance forced the Taliban to surrender Kabul, the capital, and on November 17, the Taliban confirmed that al-Qaeda military chief Mohammed Atef had been killed in the allied bombing.

Near the beginning of the war’s eighth week, on November 25, Central Intelligence Agency officer Johnny “Mike” Spann became the first combat casualty when he was killed in an uprising at Mazar-e-Sharif. Three U.S. soldiers were killed, and 19 wounded, when a U.S. bomb missed its target on December 2.

In December 2001, one dramatic phase of the war ended as the Taliban surrendered their last major stronghold in the southern city of Kandahar on December 7. Both bin Laden and Taliban leader Mullah Muhammad Omar apparently escaped from the city. December 16 saw the fall of Tora Bora, a cave complex where al-Qaeda and Taliban holdouts had hidden. Six days later, on December 22, Hamid Karzai was sworn in as chairman of a six-month interim government. Women, treated as slaves under Taliban rule, could again vote, participate in government, and receive an education.

**Early 2002: Operation Anaconda.** On January 4, 2002, U.S. Army Sergeant First Class Nathan Ross Chapman became the first member of the U.S. military to be killed by hostile fire. Fighting continued in spurts until March 2, the launch of Operation Anaconda. The largest ground operation of the war, Anaconda involved some 2,000 U.S., Afghan, and allied troops, and would result in eight U.S. deaths. Its purpose was to eliminate Taliban and al-Qaeda fighters still holding out in the mountains of southeastern Afghanistan. But as the mission came to a close some two weeks later, assessment of its success was difficult.

Over the course of an 11-day battle near Shah-i-Kot, for instance, U.S. military commanders had been forced to reassess original estimates of enemy strength in the region upward from 150 or 200 to 1,000. As that part of the offensive came to a close on March 17, it appeared that the U.S. military had produced as many as 800 enemy casualties, but numbers were difficult to determine. In any case, civilian and military leaders were not inclined to evaluate the offensive in terms of body counts—a lesson learned from the Vietnam War a generation earlier.

**Infinite Justice and Noble Eagle.** Enduring Freedom, as the larger operation came to be known in November, was initially called Infinite Justice. The change resulted from concerns that the original name had religious connotations, suggesting that God was on the side of the coalition forces. (Similarly, in the wake of the September 11 attacks, Bush had once mentioned a “crusade,” an unfortunate choice of words that played right into the terrorists’ claims that the war on terrorism was an attack by Christians against Islam.) Still, the coalition took extraordinary measures, including dropping thousands of leaflets and radio





Illegal combatants and terrorist supporters from Operation Enduring Freedom in Afghanistan being held at Camp X-Ray, on the US naval base in Guantanamo Bay, Cuba. AP/WIDE WORLD PHOTOS.

broadcasts, to assure the population of Afghanistan that the warfare was directed at eliminating al-Qaeda terrorists, not the practitioners of Islam.

Accompanying Enduring Freedom was Noble Eagle, a military operation designed to safeguard homeland security during the war in Afghanistan. The U.S. Coast Guard (USCG), principal guarantors of stateside port security, played a central role in Noble Eagle. USCG deployed 55 cutters (small armed vessels), 42 aircraft, and hundreds of boats to establish port and coastline patrols. It also called up more than 2,800 reservists to support homeland security operations at the country's 361 ports.

■ FURTHER READING:

PERIODICALS:

- "Black September 11." *Air Force Magazine* 95, no. 9 (September 2002): 46–53.
- Blumenstein, Rebecca, and Matthew Rose. "Name that Op: How U.S. Coins Phrases of War." *Wall Street Journal*. (March 24, 2003): B1.

- "Enduring Freedom." *New York Times*. (August 11, 2002): 4.
- "Military Operations Named." *Marine Corps Gazette* 85, no. 11 (November 2001): 4.
- Thompson, Loren B. "The Lessons of 'Enduring Freedom'." *Wall Street Journal*. (January 7, 2002): A24.

ELECTRONIC:

- Operation Enduring Freedom. U.S. Army. <<http://www.army.mil/operations/oef/index.html>> (April 4, 2003).
- . U.S. Navy Office of Information. <[http://www.chinfo.navy.mil/navpalib/news/news\\_stories/pentstruck.html](http://www.chinfo.navy.mil/navpalib/news/news_stories/pentstruck.html)> (April 4, 2003).
- Operations Enduring Freedom and Noble Eagle. U.S. Air Force. <<http://www.af.mil/news/efreedom/index.shtml>> (April 4, 2003).

SEE ALSO

- Bush Administration (2001–), United States National Security Policy*
- Clinton Administration (1993–2001), United States National Security Policy*
- Enduring Freedom, Operation*
- Iraqi Freedom, Operation (2003 War Against Iraq)*

*Persian Gulf War*  
*September 11 Terrorist Attacks on the United States*  
*Vietnam War*

## Energy Directed Weapons

■ LARRY GILMAN

Weapons that use energy to disable or destroy equipment or people are referred to as energy directed weapons. Examples include lasers, high-power microwave weapons, and charged particle beam weapons.

The genesis of energy directed weapons was the work of Albert Einstein. Einstein's 1905 Special Theory of Relativity related electric and magnetic forces in the equation  $E=mc^2$ . The equation demonstrated that even particles of small mass moving at the speed of light possess tremendous energy.

Energy directed weapons concentrate large amounts of energy at a specific wavelength and frequency and then direct the beam of energy at the intended target. Because the particles are moving at a speed that approaches the speed of light, the beam will have a devastating amount of energy.

**Rationale for energy directed weapons.** Those who favor energy directed weapons argue that their development would increase the ability to fight and win a conflict.

In theory, energy directed weapons would operate at or near the speed of light. Even rapidly moving missiles would be essentially motionless to the beam. For example, a missile 50 kilometers away moving at 20,000 feet per second would only move five feet from the time a energy weapon was "fired" until contact. As well, the weapons could operate over thousands of kilometers, even in space. Finally, as long as there was power to generate the high energy, no other ammunition is required.

The use of energy directed weapons in space, particularly on Earth-orbiting satellites, has been proposed. One reason is that conventional weapons do not operate well or at all in the semi-vacuum of Earth orbit. Energy directed weapons face no such limitation. Another reason is the proliferating use of space for offensive weapons. In 1972, only nine nations were known to have ballistic missiles. By 2001, this number had grown to at least 28 nations. This increase has bolstered the argument for the ability to defend and if necessary retaliate from space.

**Laser weapons.** A laser—an acronym for "light amplification by stimulated emission of radiation"—emits a tightly focused beam of specific radiation that does not diverge from the beam path. Chemical lasers use reactive energy

between compounds (i.e., oxygen/iodine and deuterium/fluoride). Solid state lasers use electricity to produce the beam. Chemical lasers currently produce much more energy than do solid-state lasers. This power, however, comes at the expense of a large volume for the great quantities of chemicals required.

High power laser light can damage or permanently destroy the eyes, and obliterate objects in its path. For example, a weapon called the Saber 203 is a "laser grenade" that is capable of temporarily blinding those in the path of the ray. The weapon was deployed, but never used with United States troops during the 1990 Gulf War, and with troops deployed to Somalia in 1995. Another weapon called the Dazer fires up to 50 laser pulses per minute. It is being used by U.S. Special Operations Command forces.

Research by the U.S. Army and Navy to develop lasers for air and sea has been underway since the early 1970s. A chemical laser weapon capable of being mounted on the next generation of fighter jet (Joint Strike Fighter) and destroyer (DDX) is scheduled to be ready for testing in 2010. As of 2002, a chemical laser was to be built aboard a modified Boeing 747 aircraft. The airborne chemical laser, which will be the first in the U.S., is controversial because of the possibility of environmental damage from the chemicals carried aboard the aircraft.

Military use of lasers is currently confined to low-power units that measure the distance to a target or help aim other weapons. Lasers could become much more formidable weapons. For example, experts agree that a 25 to 100 kilowatt laser would be powerful enough to disable equipment hundreds of miles away, and could burn through metal, such as the outer casing of a missile, dozens of miles away.

**High-power microwave weapons.** High-power microwave (HPM) weapons are also known as Radio Frequency weapons and Ultra-Wideband weapons. HPM weapons have been in development by the United States, Russia, China, and other countries for decades. The weapons produce high-energy bursts; a typical HPM weapon consists of a power source that can be electrical or explosive, a microwave generator, and an antenna to direct the beam of radiation. The intense surge of energy that is emitted disables electronics in vehicles, communications equipment, and other weapons. Such a weapon was successfully field tested by the U.S. in April 2001.

**Particle beam.** Development of the particle beam weapon (PBW) began in the U.S. in the late 1950s, under the code name Seesaw. A PBW operates by accelerating components of a hydrogen atom—either the negatively charged electron or the positively charged proton—to almost the speed of light, and then focusing these atoms into a beam. The destructive power of the particle beam is due to the collision of the positively or negatively charged ions with



A U.S. Navy pilot inspects the laser guided weapons aboard his F/A-18C Hornet prior to his mission from the aircraft carrier USS *Theodore Roosevelt*. AP/WIDE WORLD PHOTOS.

the atoms of the target. The energy transfer causes an explosion, which obliterates the target.

The charged version of a particle beam weapon would be utilized where there is an atmosphere. The neutral particle beam weapon, which is not as powerful, is more suitable to the friction-free atmosphere of space, where it retains enough power to be destructive. A space version of a PBW does not yet exist. Among the developmental limitations is an aiming system capable of accuracy over thousands of kilometers, and the maintenance of a tightly focused beam over such vast distances (a beam composed of like-charged particles will tend to broaden out, as the particles repel one another).

**Limitations and criticisms of energy directed weapons.** Because energy directed weapons are beamed at the target, they are “line of sight” weapons. Unless technological changes allow the beams to be precisely bent or reflected, objects that are not directly in front of the beam will not be targeted. In contrast, a conventional weapon such as bomb can destroy its target even when the weapon is slightly off the intended destination. Furthermore, laser beams are blocked by clouds, limiting their use to all but fair weather.

Those who oppose energy directed weapons argue that civilian casualties and infrastructure damage will be greater than with the present methods of warfare. Also the weapons could be an ideal terrorist tool. The source of

energy directed weapons could be disguised, and no traces are left behind.

The collateral effects of energy directed weapons such as lasers are still unclear. While an enemy target would certainly be disrupted or even destroyed, the possibility of damage to civilian structures (i.e., equipment in hospitals) or civilians themselves (i.e., disruption of pacemakers) has made the deployment of energy directed weapons controversial. Even if the energy weapon can be contained in a relatively narrow beam prior to the strike, dispersion of the energy at ground level will likely occur. It is this traveling shock wave of energy that could produce the collateral damage.

#### ■ FURTHER READING:

##### BOOKS:

Duffner, Robert. *Airborne Laser: Bullets of Light*. New York: Plenum Trade, 1997.

##### ELECTRONIC:

In These Times. “Now You See, Now You Don’t.” The Institute for Public Affairs. September 27, 2002. <<http://www.inthesetimes.com/issue/26/24/news1.shtml>>(17 December 2002).

Lexington Institute, 1600 Wilson Boulevard, Suite 900, Arlington VA 22209. (703) 522-5828. <[http://www.lexingtoninstitute.org/defense/energyforum\\_thompson.htm](http://www.lexingtoninstitute.org/defense/energyforum_thompson.htm)>.

## SEE ALSO

DARPA (Defense Advanced Research Projects Agency)  
*Electromagnetic Weapons, Biochemical Effects*  
 Lawrence Livermore National Laboratory (LLNL)

## Energy Regulatory Commission, United States Federal

The U.S. Federal Energy Regulatory Commission (FERC) is an independent regulatory agency within the Department of Energy (DOE) responsible for regulating energy utilities nationwide. As such, it has a significant oversight role in America's critical infrastructure. In the aftermath of the September 11, 2001, terrorist attacks, FERC has worked to help ensure protection of information concerning energy utilities.

FERC is responsible for regulating, in interstate commerce, the transmission of oil by pipeline, the transmission and sale of natural gas for resale, and the transmission and wholesale sales of electricity. It also licenses and inspects private, municipal, and state hydroelectric projects, approves site choices, and plans for abandonment, of interstate pipeline facilities; and oversees environmental issues as these relate to natural gas, oil, electricity, and hydroelectric power projects. Additionally, FERC administers the accounting and financial reporting regulations, and the conduct of jurisdictional utility companies.

At the time the Department of Energy Organization Act established DOE on October 1, 1977, the national utilities oversight organization was known as the Federal Power Commission (FPC). The FPC was later disbanded and FERC established in its place. FERC's membership comes from five presidential appointees, no more than three of whom may belong to the same political party. Its members, whose appointments are made with the advice and consent of the Senate, serve terms of five years. Although there is a chairperson designated by the president, all members have equal voting power.

In the atmosphere of heightened security consciousness that emerged after the September, 2001 terrorist attacks, FERC has worked with entities in the private and public sectors to ensure greater protection of interstate utilities. In September 2002, FERC proposed new rules limiting public access to information on power plants, pipelines, and other aspects of critical infrastructure as it relates to energy. Information that had been easily available on its Web site would thenceforth be granted purely on a need-to-know basis.

## ■ FURTHER READING:

## PERIODICALS:

"FERC Streamlining to Reflect Industry." *Oil & Gas Journal*. 96, no. 26 (June 29, 1998): 33.

Gips, Michael A. "They Secure the Body Electric." *Security Management* 46, no. 11 (November 2002): 77–81.

Matthews, William. "Energy Agency Says Web Info Poses Threat." *Federal Computer Week* 16, no. 34 (September 23, 2002): 46.

## ELECTRONIC:

Federal Energy Regulatory Commission. <<http://www.ferc.fed.us/>> (February 23, 2003).

## SEE ALSO

*Critical Infrastructure Assurance Office (CIAO), United States*  
*DOE (United States Department of Energy)*

## Energy Technologies

## ■ LARRY GILMAN

Energy technologies are techniques for moving energy from a source to a point of use, for transforming it from an original source-form to an end-use form, or both. They are often lumped into two groups, conventional and alternative. Conventional energy technologies derive energy from fuels, either fossil (coal, oil, natural gas) or nuclear (uranium, plutonium). These technologies first turn the energy latent in fuel into heat, then transform some percentage of that heat into another, more useful form of energy (or apply the heat directly, as to warming a building, smelting ore, or the like). Approximately 90% of present-day energy use is provided by conventional sources.

Alternative energy technologies, in contrast, harvest energy from renewable, natural flows rather than from fuels. Technologies that collect energy from sunlight, wind, wave action, or plants are considered alternative energy technologies. (An exception to the alternative/conventional classification scheme is hydroelectric power, the generation of electricity from water flowing downhill. Hydroelectric power, although it harvests an energy flux from the environment rather than burning a fuel, is usually considered conventional because it has been utilized on an industrial scale for so long.)

Many energy technologies, conventional and alternative, produce electricity. Electricity is a uniquely useful form of energy, not a source of energy. Thus, the belief that an electric-powered device such as an electric car is "clean" is only correct when the electricity that it uses is produced cleanly. Most electricity is produced by coal-burning power plants or nuclear power plants; the former

involves environmentally destructive mining and air pollution, while the latter involves some environmentally destructive mining and produces growing inventories of radioactive material that might be released to the environment either accidentally or deliberately, as by wartime or terrorist action. Therefore, there is nothing intrinsically “clean” about electricity. About 51% of United States electricity is currently produced by coal-burning power plants, 21% by nuclear power plants, 17% by natural-gas-fired power plants, 6% from hydroelectric dams, 3% from oil-fired power plants, and 2% from wind, wood, and photovoltaics.

Several national-security issues arise with respect to energy technologies:

(1) *Self-sufficiency.* An energy source that must be imported, such as oil, is vulnerable to cutoff by hostile parties. This was demonstrated by the oil crisis of 1973, when the Organization of Oil Producing Countries (OPEC) suddenly quadrupled its oil prices from about \$3 to about \$13 per barrel (1 barrel = 42 United States gallons or 159 L) in retaliation for United States support of Israel. This triggered an economic crisis in the United States and elsewhere. In contrast, the United States has large domestic stocks of coal and uranium, and is not vulnerable to a cutoff of these energy sources; nor is it entangled politically or militarily with foreign sources of these fuels, as is the case with oil. (However, coal and uranium produce electricity, which, unlike oil, does not yet run affordable cars; therefore, coal and uranium cannot, at present, significantly decrease United States dependence on foreign oil.) Renewable or alternative energy resources also have the advantage that they are not imported.

(2) *Fragility.* Energy sources that can be disrupted at central points or along key transmission routes are more vulnerable to terrorism and war than distributed energy sources. For example, much of the United States electrical grid—a tuned, interdependent, dynamic network—could be blacked out for days or weeks by the destruction of relatively few switching points, control centers, or transmission lines. Locally-harvested alternative-energy sources such as rooftop photovoltaics or woodlots are immune to large-scale disruption, but cannot serve all purposes; rooftop photovoltaics are still expensive relative to grid electricity, and there are no wood-burning computers or refrigerators. Between the resilience of locally-produced energy supplies and the brittleness of the coal- and nuclear-fueled electrical grid lie the energy systems that rely on distributed stocks of fuels such as gasoline and natural gas. Although these energy technologies still rely on a few centralized refineries or long-distance pipelines, they are tolerant of temporary or local damage.

(3) *Hazardousness.* Some energy sources are hazardous due to toxicity or explosive potential. Standard nuclear power plants cannot explode, but they do contain large inventories of radionuclides that could be deliberately released by an enemy; after the terrorist attacks of

September 11, 2001, the United States Nuclear Regulatory Commission ordered immediate, drastic increases in security for nuclear power plants. A less well-known source of vulnerability is liquefied natural gas, which is imported to the United States in large tanker ships and stored in centralized tank farms for national distribution via long-distance pipelines.

(4) *Pollution.* Pollution or greenhouse-gas emissions that harm a country’s citizens, environment, and economy can be thought of as a danger to national security. All sources of energy, including wind and solar, require the extraction and refinement of metals and other substances, some toxic; conventional sources further require the extraction and (often) refinement of fuels and either (a) release combustion products to the atmosphere or (b) require the near-perfect, near-perpetual containment of increasing quantities of radioactive materials.

(5) *Adequacy.* Whatever combination of energy technologies is used by a modern industrial state, its energy system must provide *sufficient* energy. The present energy system of the U.S.—primarily gasoline for transport, coal and nuclear (primarily) for electrical generation, and oil for heating some buildings—does supply adequate energy; however, some experts maintain that given increased end-use efficiency, the industrialized countries could shift almost entirely to alternative energy sources in about 50 years. If technically feasible this would increase self-sufficiency and decrease fragility, hazardousness, and pollution, but is not likely to occur without a major shock, or several major shocks, to the conventional energy system, as for example a major terrorist act involving a nuclear power plant, a second oil embargo, or radical climate change. In the meantime, prices are falling slowly for alternative energy sources, especially wind and solar, making them increasingly competitive on the market with conventional electricity sources. Gasoline continues to be the only affordable energy source for most vehicles, with the mileage of the United States fleet recently declining rather than rising.

One change in the present U.S. energy system that, if technically feasible, would increase self-sufficiency by decreasing dependence on oil and which would also decrease pollution is a long-term shift (probably only partial) to hydrogen “burned” in fuel cells. Fuel cells are chemical reactors in which a fuel (not necessarily hydrogen) combines with oxygen to create electricity, with water vapor as the only by-product. Hydrogen is available on Earth only in chemically stable combination with other substances (e.g., in H<sub>2</sub>O); it is therefore not a primary fuel but, like electricity, a *form* of energy, and must be manufactured either by using electricity to split water molecules or by chemical processing of a fuel such as coal. Although hydrogen is not currently available in large quantities and fuel cells remain expensive (i.e., about 10 times as expensive, per horsepower delivered, as a conventional automobile engine), U.S. President George W. Bush has announced two funding programs for hydrogen fuel cells:

Freedom Car (2002) to accelerate development of hydrogen-powered automobiles, and Freedom Fuel (2003), to accelerate development of techniques for manufacturing hydrogen from coal. Freedom Car receives about \$50 million per year, and Freedom Fuel has been allotted \$144 million per year for five years. The announced goal of the twin programs is to make fuel-cell powered cars commercially available in 20 years. The United States is working in partial cooperation with the European Union, which also seeks to develop hydrogen-powered fuel cells for cars. The European Union's program, unlike the U.S. Freedom Fuel program, seeks to produce hydrogen using electricity generated by wind and solar power.

#### ■ FURTHER READING:

##### BOOKS:

Brockris, J. O'M. *Energy Options*. Redfern NSW, Australia: Halsted Press, 1980.

Lovins, Amory, and L. Hunter Lovins. *Brittle Power: Energy Strategy for National Security*. Andover, MA: Brick House Publishing, 1982.

##### PERIODICALS:

Banerjee, Neela. "U.S. and Europe in Fuel Cell Pact." *New York Times*. March 7, 2003.

##### SEE ALSO

*DOE (United States Department of Energy)*

## Engraving and Printing, United States Bureau

The United States Bureau of Engraving and Printing (BEP) is the largest producer of security documents in the nation. Although it is most widely known for the production of Federal Reserve notes, paper currency is only one of many printed materials that originate from its facilities in Washington, D.C., and Fort Worth, Texas. BEP is also responsible for printing postage stamps, identification cards, Treasury securities, and other sensitive documents.

**Background.** BEP had its beginnings in 1862, when a small room in the basement of the Treasury building in Washington was set aside for the separating and sealing, by hand, of United States \$1 and \$2 notes printed by private companies. Over time, BEP's mission expanded as it began to produce some currency notes, as well as revenue



Former Treasury Secretary Paul O'Neil, left, looks at newly-printed bills with a Bureau of Printing employee during a tour of the Western Currency facility in Fort Worth, Texas. AP/WIDE WORLD PHOTOS.

stamps, certificates recording obligations of the U.S. government, and a variety of other security documents authorized by various governmental departments. BEP became the sole authorized producer of U.S. paper currency in 1877, and in 1894 began producing postage stamps.

By 1985, officials at the Treasury Department had become aware of the need for a BEP facility west of the Mississippi River, which would reduce the cost of transporting notes to Federal Reserve banks in San Francisco, Dallas, and Kansas City. Treasury therefore authorized BEP officials to accept proposals from potential host cities, for which there were 83 applications. In November 1986, BEP chose Fort Worth, and in 1987 began building what is today known as the Western Currency Facility. The design of the building, which in 1991 received an award from the local chapter of the American Institute of Architects, includes a glass pyramid intended to replicate the truncated pyramid on the reverse side of a one-dollar bill.

**Production.** Today BEP continues to produce all paper money in the United States, while the United States Mint produces all coins. Both distribute their products solely through the Federal Reserve System, which in turn issues

currency and coinage solely through member financial institutions. BEP is also responsible for the processing of claims for the redemption of mutilated currency. Its research and development department is concerned with anti-counterfeiting technology, which is perpetually upgraded in an effort to remain many steps ahead of counterfeiters.

Although the production of U.S. currency is perhaps the most visible of BEP's activities, it is far from the only one. BEP produces a number of stamps and notes, including postage stamps for the United States Postal Service, license stamps such as those used on alcohol products, and Treasury securities. The lowest-value note ever issued by BEP was a \$0.002, or one-fifth cent, wine stamp, while the item of highest value was a \$100,000,000 International Monetary Fund special note. BEP has also manufactured currency for other nations, including pre-Communist Cuba.

BEP produces federal identification cards, certificates of naturalization, and other security documents as requested by particular government agencies. Among its most specialized products are engraved White House invitations.

#### ■ FURTHER READING:

##### BOOKS:

*History of the Bureau of Engraving and Printing, 1862–1962.* Washington, D.C.: Treasury Department, 1964.

*The Money Factory.* Washington, D.C.: Bureau of Engraving and Printing, 1993.

Sincerbox, Glenn T. *Counterfeit Deterrent Features for the Next-Generation Currency Design.* Washington, D.C.: National Academy Press, 1993.

##### ELECTRONIC:

Bureau of Engraving and Printing. <<http://www.bep.treas.gov/>> (February 5, 2003).

##### SEE ALSO

*Counterfeit Currency, Technology and the Manufacture Federal Reserve System, United States Treasury Department, United States*

---

## Engulf, Operation

---

#### ■ JUDSON KNIGHT

Engulf was a series of operations whereby the British Security Service, MI5, intercepted Egyptian and French cipher transmissions during a period from the mid-1950s to the mid-1960s. The first major operation of Engulf took place during the Suez crisis of 1956, when a team led by British spymaster Peter Wright planted a bug in the cipher room of the Egyptian embassy in London.

The Suez crisis began in July 1956, when Egyptian president Gamal Abdel Nasser seized the Suez Canal, formerly under the control of Britain and France. Britain and the United States, well aware of Nasser's increasingly close ties with the Soviet Union, had refused to fund Nasser's plans to build the Aswan High Dam. Therefore, Nasser took over the canal, not only as an act of retaliation, but as a means of raising money by collecting the tolls charged to ships passing through the canal. Britain and France, in a plan orchestrated with Israel, forced the evacuation of Egyptian troops, but were ultimately forced to themselves evacuate by the threat of United Nations or Soviet intervention.

In the months leading up to the crisis, MI5 undertook efforts to plant a listening device (bug) in the Egyptian embassy. The British postal service, which controlled telephone service, deliberately created problems with the embassy's phones, and an MI5 undercover team arrived under the guise of repairing the equipment. While there, they planted bugs that allowed them to hear the noises made by the setting of the machines. Skilled specialists were able to translate these noises into usable intelligence.

**An unexpected conduit from Moscow to London.** As Wright later recalled in his autobiography *Spycatcher*, intercepting the Egyptian cipher transmissions allowed MI5 to follow discussions between the Egyptians and Soviets in Moscow, the specifics of which were regularly passed on to the embassy in London. From these transmissions, the British learned that the Soviets were not simply bluffing when they threatened to intervene in Suez on the Egyptians' behalf.

Wright went on to recount that the Soviets helped their Egyptian allies by sweeping the London embassy for bugs, but when they discovered the device planted by MI5, they opted to leave it in place and not inform the Egyptians. By allowing MI5 to listen in to the Egyptian embassy, the Soviets were able to convey exactly where they stood on the Suez situation, and to do so in such a way that the British would know that they meant what they were saying.

**Other phases.** In later phases of Engulf, MI5 attempted to detect cipher noises in other contexts. In 1959, for instance, while the Soviet cruiser *Ordzhonikidze* was moored at Stockholm, Sweden, MI5 placed microphones in a nearby warehouse. This time, of course, there was no question of going aboard the ship under any pretext to plant a bug, and as it turned out, the warehouse was not close enough. Though MI5 did pick up what were apparently cipher machine noises, this did not lead to any usable intelligence.

From 1960 to 1963, in an operation known as Stockade, MI5 listened in to the French embassy in London. Unlike the Suez phase, however, reliable intelligence did not give the British any real diplomatic benefit. The United

Kingdom was attempting to join the European Economic Community (EEC) or Common Market, which in 1993 would become the European Union. France was attempting to keep Great Britain out of the EEC, and the bugging simply revealed that the French were not going to budge, without revealing any likely means of inducing them to do so. Wright, who also led Stockade, later recalled that the operation “was a graphic illustration of the limitations of intelligence.”

#### ■ FURTHER READING:

##### BOOKS:

- Aldrich, Richard J. *The Hidden Hand: Britain, America, and Cold War Secret Intelligence*. Woodstock, NY: Overlook Press, 2002.
- Epstein, Leon D. *British Politics in the Suez Crisis*. Urbana: University of Illinois Press, 1964.
- Kelly, Saul, and Anthony Gorst. *Whitehall and the Suez Crisis*. Portland, OR: Frank Cass, 2000.
- Louis, William Roger, and Roger Owen. *Suez 1956: The Crisis and Its Consequences*. New York: Oxford University Press, 1989.
- West, Nigel. *The Circus: MI5 Operations 1945–1972*. New York: Stein and Day, 1983.
- Wright, Peter. *Spycatcher: The Candid Autobiography of a Senior Intelligence Officer*. New York: Viking, 1987.

##### SEE ALSO

- Cipher Machines*  
*Egypt, Intelligence and Security*  
*MI5 (British Security Service)*  
*Special Relationship: Technology Sharing Between the Intelligence Agencies of the United States and United Kingdom*  
*United Kingdom, Intelligence and Security*

## ENIAC Machine.

SEE *Ultra, Operation*.

## Enigma

#### ■ LARRY GILMAN

Enigma was a ciphering (code communication) system used by the German military from 1926 until the end of World War II, and by several other nations for some years after. Enigma was the first mechanized message-encryption system to see wide use. Enigma produced such thoroughly scrambled messages that for many years its cipher

was considered unbreakable both by the German military and its foes. Polish and British mathematicians, however, cracked the Enigma cipher in time to give the Allies access to most German military communications throughout World War II. The German government never knew that the Enigma cipher had been broken and that its military communications were often transparent, giving a significant advantage to the Allies on many occasions. The Japanese military also used a cipher related to Enigma during World War II. The Japanese version of Enigma was cracked by American cryptographers, providing a crucial advantage to the Allies in the Pacific theater. U.S. knowledge of secret Japanese transmissions was essential, for example, to victory at the crucial battle at Midway, the Japanese navy’s first major defeat in several centuries. Many military strategists and historians hold that Allied success in cracking the Enigma and related ciphers helped significantly shorten World War II.

**Origin of Enigma.** During World War I, cumbersome paper-and-pencil ciphers were still the rule, as they had been for centuries past. (A *cipher* is any scheme for transforming ordinary written language—*plaintext*—into a coded, but apparently random string of characters, *ciphertext*.) After World War I, several inventors turned their attention to the mechanization of ciphering, seeking to increase accuracy, speed, and security. The most successful of these inventors was German engineer Arthur Scherbius, who in 1918, created a cipher machine he named the Enigma. (This is not a translation; the word “enigma” is the same in German and English). Scherbius was unsuccessful in selling Enigma to commercial buyers. It was not until 1923 that Enigma was chosen by the German government as its standard ciphering system, as Germany had only just learned how much damage had been done by the breaking of its ciphers by the Allies in World War I. Between 1925 and 1945, the German military bought over 30,000 Enigma machines, deploying slightly different systems to its European armies, its army in North Africa, its air force, and its navy.

**The Enigma cipher.** The Enigma cipher is built upon the simplest of all cipher types, the substitution cipher. In a substitution cipher, one letter of the alphabet is substituted directly for another. A substitution cipher for a six-letter alphabet might appear as:

Plaintext:	A B C D E F
Ciphertext:	F C A B D E

Using this cipher, the plaintext word BAD (for example) would produce the ciphertext word CFB. Such ciphers are easy to implement, but also contain easily broken code, as their ciphertext contains all the regularities of





A four-rotor Enigma machine, right, which was used by the crews of German U-boats in World War II to send coded messages. AP/WIDE WORLD PHOTOS.

ordinary language: that is, double letters in plaintext appear as double letters in ciphertext, the ciphertext letter for “e” will appear in the ciphertext just as often as “e” appears in plaintext, and so forth. Such codes are weak because analyzing regularities is one of the primary means by which codebreakers attack codes.

However, by adding complications to this simple idea, a powerful code can be devised. Consider the following substitution cipher for a three-letter alphabet:

Plaintext:	A B C
Ciphertext:	A C B

In this simple example, A is enciphered as itself. This cipher can be imagined as a physical device consisting of three disks or dials arranged in a row. The first (left-hand) and third (right-hand) disks, each of which has the alphabet ABC spaced evenly around its edge, are identical, and are aligned so that their letters are in the same positions; the third disk, which sandwiched between the other two, is different. It contains three wires that pass from its left side right through to its right, connecting the two alphabet disks so that the A of the left-hand disk is wired to the A of the right-hand disk, the B of the left-hand disk to the C of

the right-hand disk, and the C of the left-hand disk to the B of the right-hand disk. In effect, the middle disk scrambles the alphabet. The result is a simple substitution cipher. If the middle disk, (the scrambler) is rotated, however, so that the wire which touched A on the plaintext disk now touches C on that disk, all the other letters on the plaintext and ciphertext disks will also be connected differently by the scrambler, producing the following substitution cipher:

Plaintext:	A B C
Ciphertext:	B A C

This can be verified by describing the wires in the scrambler as a set of input-output rules, one for each wire:

- 1) Connect input position 1 to output position 1.
- 2) Connect input position 2 to output position 3.
- 3) Connect input position 3 to output position 2.

By rule 1, when scrambler input position 1 is lined up with the letter A on the left-hand (plaintext) disk, it is connected to output position 1, which is lined up with the

letter A on the right-hand (ciphertext) disk. The other two substitutions are produced by the other two wires: B → C, C → B. When the scrambler is rotated so that its input 1 moves from A to C on the plaintext disk, its output 1 moves from A to C on the ciphertext disk. Now, instead of producing A → A, wire 1 produces C → C. The other two wires now produce the substitutions A → B, B → A. Thus, each time the scrambler is rotated by one letter position, a new different substitution code is produced. This continues until the scrambler returns to its starting position, whereupon the substitution codes produced by the device begin to repeat. In this example, repetition begins with the third shift of the scrambler.

Rotation of the scrambler can be used to make a cipher that is more formidable than a straightforward substitution. Consider a three-letter plaintext message is to be sent: ABA. First, A is enciphered with the scrambler in the first position described above: A → A. Before the second letter is encrypted, the scrambler disk is rotated by one letter-position. The second plaintext letter is then enciphered: B → A. The disk is rotated, and A is enciphered again: A → C. Although in this case one would start repeating substitutions after only three letters, the resulting cipher is significantly more complex, and thus harder to crack, than a static substitution cipher.

Decryption in this system is simple as long as the receiving party possesses an identical machine; the wires in the scrambler disk work equally well in either direction, so decryption is simply encryption run backwards. The receiver must, however, begin decrypting with their scrambler set to the same position as the sender's at the start of transmission, otherwise the substitution codes used by the receiver to decipher the message will be out of step with those used by the sender to encipher it, and decipherment will fail.

The Enigma system was based upon the scrambler-disk principle described above. Enigma used not a 3-letter, but a 26-character alphabet and not one, but four scrambler disks. The first scrambler scrambled plaintext or ciphertext, the second scrambler scrambled the outputs of the first scrambler, the third scrambled the outputs of the second, and the fourth fed back, or "reflected," the outputs of the third so that messages passed through the other three scramblers before the encrypted ciphertext (or decrypted plaintext) was read. Each letter was thus scrambled a total of seven times during its passage through the machine. Three of the scrambler disks could be rotated freely, but the fourth, the "reflector," was stationary.

In order to use an Enigma unit, its operator typed plaintext or ciphertext into a keyboard. For each keystroke typed, Enigma automatically shifted one or more of its scramblers and lit up a letter on a display board. The letter on the display board showed the output text for the typed input letter: ciphertext if plaintext was input, plaintext if ciphertext was input. To produce further scrambling between ciphertext and plaintext, each Enigma also had a

built-in commutator or "plugboard" that enabled the operator to crisscross paired letters of the alphabet before their signals fed into the first scrambler disk. The result was that Enigma had over 10<sup>20</sup> different "keys" or distinct settings of scramblers and plugboard. Simply guessing the correct key for a given message was, therefore, essentially impossible. Every day at midnight, all operators of a given Enigma system would switch to a new key; these initial daily keys were printed in a codebook that was distributed to the operators. For added security, the scrambler-disks part of the key was changed for every single message sent; this message-key information was transmitted twice at the beginning of every message. This technique was intended to prevent message loss due to transmission errors, but in fact reduced Enigma's effectiveness by introducing an element of predictability.

**The defeat of Enigma.** Enigma was long considered impossible to crack. However, in 1931, a disgruntled German ex-officer gave drawings for the machine to the French secret service. The French, who considered Enigma too tough to crack even with this information in their possession, gave it to the Polish government. Polish mathematician Marian Rejewski (1905–1980) used it to devise automatic devices (specialized electromechanical calculators) for re-cracking the ever-changing Enigma cipher on a daily basis. Just before the fall of Poland in 1939, Rejewski's findings were transferred to the British government, which continued to improve them.

During World War II, the German military modified the Enigma system at intervals, requiring the British to continue re-cracking the cipher throughout the war. With the help of a motley team of crossword-puzzle experts, bridge devotees, chess champions, mathematicians, and linguists led by British mathematician and computing pioneer Alan Turing (1912–1954), the group succeeded. Tragically, however, Turing was persecuted after the war for his homosexuality. His security clearance was revoked, he was forced to undergo debilitating hormone treatments, and he was banned from the development of the digital computer. Turing committed suicide in 1954, some 20 years before his crucial contribution to the cracking of Enigma, and thus, to the Allied victory, was declassified.

#### ■ FURTHER READING:

##### BOOKS:

Churchouse, Robert. *Codes and Ciphers*. Cambridge, England: Cambridge University Press, 2002.

Singh, Simon. *The Code Book*. New York: Doubleday, 1999.

##### SEE ALSO

*Cipher Machines*  
*Codes and Ciphers*

## Entry-Exit Registration System, United States National Security

The U.S. National Security Entry-Exit Registration System (NEERS) is a program whereby persons whose nationality identifies them as a possible security risk are required to submit to control processes governed by the U.S. Department of Justice. Established in June, 2002, the system is a response to the September 11, 2001, terrorist attacks and the increased awareness of terrorism and homeland security that emerged in their wake. Despite these concerns, some critics have charged that NEERS is unconstitutional.

On June 5, 2002, the Justice Department introduced the new system that focused on citizens of Iran, Iraq, Libya, Sudan, and Syria. In addition, "certain nationals of other countries whom the State Department and the INS [Immigration and Naturalization Service] determine to be an elevated national security risk" would be placed under the program, which required these individuals to undergo fingerprinting, photographing, and registration. Exit controls built into the system would make it easier for law-enforcement officials to monitor foreign nationals as to the length of their visas, and to ensure the removal of those who had overstayed theirs.

In the first year, NEERS would track some 100,000 foreigners, but over time it would be expanded to include the more than 35 million who visit the United States every year. Though the program's original regulations made little reference to gender, it was clear that males from teen age to middle age were the focus. By early 2003, this had been spelled out in regulations that cited males 16 and over from some 25 countries.

Almost immediately, the program invoked the ire of groups representing civil liberties interests, foreigners, or other constituencies. In December, 2002, the *Financial Times* reported that some 700 men and boys in southern California had been detained for several days on suspicion of criminal activity. Such actions, the British paper warned, could deter foreign nationals from registering with the program.

This was one legitimate concern with the program that law-abiding foreigners would register, while those for whom NEERS was created would manage to avoid the system. Some workers fled to other countries, as the *Washington Post* showed in a report on Pakistanis making their way north to Canada—only to be met with an unfriendly reception there. As for the claim that the program unfairly singled out Middle Easterners or Muslims, defenders of NEERS pointed out at least three-quarters of the terrorist attacks worldwide over the past quarter-century—including the most violent attack in September, 2001, had been perpetrated by males from the Islamic world.

### ■ FURTHER READING:

#### PERIODICALS:

Brown, DeNeen L. "Pakistanis Find Cool Reception in Canada." *Washington Post*. (March 19, 2003): A24.

Lardner, George, Jr. "Congress Funds INS Registration System but Demands Details." *Washington Post*. (February 15, 2003): A18.

Parkes, Christopher. "Anti-Terror Programme in U.S. Runs into Controversy." *Financial Times*. (December 20, 2002): 8.

#### ELECTRONIC:

Attorney General Prepared Remarks on the National Security Entry-Exit Registration System. U.S. Department of Justice. <<http://www.usdoj.gov/ag/speeches/2002/060502agpreparedremarks.htm>> (March 24, 2003).

Fact Sheet: National Security Entry-Exit Registration System. U.S. Department of State International Information Programs. <<http://usinfo.state.gov/topical/pol/terror/02060509.htm>> (March 24, 2003).

National Security Entry-Exit Registration System (NEERS). <<http://fpc.state.gov/16739.htm>> (March 24, 2003).

#### SEE ALSO

*INS (United States Immigration and Naturalization Service) Profiling*  
*September 11 Terrorist Attacks on the United States*

## Environmental Issues Impact on Security

### ■ WILLIAM C. HANEBERG

The relationship between environmental issues and national security includes the possibility of conflict over scarce resources such as fresh water and arable land, the influence of global climate changes on the types and locations of future conflicts, and the degree to which the environmental consequences of domestic military and security activities should be open to public scrutiny. Although there is no standardized definition, aspects of national security that are driven by or that address environmental issues can be collectively described by the term environmental security. Because environmental security issues are tied as closely to public policy, politics, and economics as they are to science and engineering, discussions of either are often contentious and highly polarized.

Increasing concerns about environmental quality and degradation during the past several decades have led to the incorporation of environmental elements into national security policy. Some policy scenarios, for example, discuss the possibility of United States troops invading South American countries to enforce bans against logging in rainforests or to quell violence arising from competition

for arable land and fresh water in African regions undergoing desertification. It has also been suggested that potential global warming may shrink the northern polar ice cap and open parts of the Arctic Ocean as a military theatre for surface ships as well as an avenue of commerce.

With regard to their potential for political upheaval or war as a consequence of environmental problems, the least stable parts of the world have been identified as North Africa, the sub-Saharan Sahel region of Africa (including Ethiopia, Sudan, Somalia, Mali, Niger, and Chad), the island nations of the western Pacific Ocean, the Ganges River basin (principally northeastern India and Bangladesh), and some parts of Central and South America. Some portions of Africa, in particular, do not possess resources (especially food, water, and energy) adequate to support the current population under existing conditions. Other areas are those in which climate change or continuing population growth may cause the carrying capacity of the environment to be exceeded. In either case, regional deprivation and political unrest may have global consequences if they provide an atmosphere that allows extremist or terrorist groups to flourish. Environmental security concerns will likely require the shaping of events through diplomatic efforts to promote regional stability (including the equitable provision of foreign aid); limited military response in cases where diplomatic efforts to promote stability have failed; and continuing preparation of diplomatic, military, and civilian personnel to deal with environmental security issues.

The environmental impacts of military activities and the effects of domestic environmental laws on military readiness are also evolving concerns. Like other federal agencies, the Department of Defense has historically complied with the National Environmental Policy Act (NEPA) that requires, for example, the preparation of Environmental Impact Statements (EIS) or Environmental Assessments (EA) prior to many activities. Military facilities are also required to develop Integrated Natural Resources Management Plans (INRMPs) that must be revised every five years. In order to decrease the operational and budgetary impacts of environmental laws on military activities deemed essential to national security, the Strategic Environmental Research and Development Program (SERDP), a Department of Defense program, was established in 1990. Its focus areas include the development of more effective methods and technologies for the cleanup of contaminated military sites, compliance with environmental laws and regulations, conservation of natural resources, pollution prevention, and identification and destruction of unexploded ordnance. More recently, the Department of Defense has sought military exemptions from environmental laws that include the Endangered Species Act, the Clean Air Act, the Clean Water Act, and the Marine Mammal Protection Act. The House Armed Services Committee voted in 2002 to allow the Department of Defense to ignore some environmental laws, but compromise legislation passed several months later in the Senate limited this to a temporary exemption from the Migratory Bird

Treaty Act. The legislation also directed the secretary of the interior to draft within one year regulations that would permanently exempt many military activities from environmental laws.

#### ■ FURTHER READING:

##### BOOKS:

King, Chris. *Understanding International Environmental Security: A Strategic Military Perspective*. AEPI-IFP-1100A. Atlanta, GA: Army Environmental Policy Institute, 2000.

Petzold-Bradley, E., A. Carius, and A. Vincze (editors). *Responding to Environmental Conflicts: Implications for Theory and Practice*. Dordrecht, The Netherlands: Kluwer Academic Publishers, 2001 .

Price-Smith, A. T. *The Health of Nations: Infectious Diseases, Environmental Change, and Their Effects on National Security and Development*. Cambridge, MA: MIT Press, 2001 .

##### ELECTRONIC:

Benjamin, Paul. "Green Wars: Making Environmental Degradation a National Security Issue Puts Peace and Security at Risk." The Cato Institute, Policy Analysis No. 369. April 20, 2000. <<http://www.cato.org/pubs/pas/pa-369es.html>> (14 March 2003).

Pacific Institute. "Environment and Security." <[http://www.pacinst.org/environment\\_and\\_security/](http://www.pacinst.org/environment_and_security/)>(14 March 2003).

Pike, John. "Environmental Issues." December 12, 2002. <<http://www.globalsecurity.org/military/facility/environment.htm>>(14 March 2003).

Strategic Environmental Research & Development Program. "Welcome to SERDP." March 10, 2003. <<http://www.serdp.org/>>(14 March 2003).

U.S. Army Corps of Engineers. "NEPA and Army Management." September 10, 2002. <<http://aec.army.mil/usaec/nepa/compliance00.html>>(14 March 2003).

##### SEE ALSO

*EPA (Environmental Protection Agency)*  
*Food supply, Counter-Terrorism*  
*Natural Resources and National Security*  
*Water Supply: Counter-Terrorism*

---

## Environmental Measurements Laboratory

---

#### ■ K. LEE LERNER

The Environmental Measurements Laboratory (EML) is a research laboratory located in New York City, first established in 1947, that is operated by the United States

government. Research at the facility is coordinated by the Science and Technology (S&T) Directorate of the Department of Homeland Security. EML scientists are an integral part of the nation's radiological incident emergency response plans.

As a federal laboratory, EML supports the United States Department of Energy (DOE) National Security objectives. EML responsibilities include monitoring international compliance with nonproliferation treaties. EML is a part of the Homeland Security Monitoring Network (HSMN) and is also an official U.S. Radionuclide Laboratory with facilities dedicated to support of the International Monitoring System.

EML programs are designed to develop and train personnel in instruments and technologies capable of detecting radioactive substances and identifying nuclear threats. EML has advanced programs in radiation survey planning, radiological monitoring and assessment, and radiation measurements (including dosimetry measurements). EML also hosts high resolution gamma sensors and equipment dedicated to measuring environmental radiation and radioactivity.

Unique EML research capabilities include the ability to generate atmospheric conditions that allow experimental evaluation of instrumentation. EML scientific programs include collaborative research with global meteorological groups dedicated to developing more accurate atmospheric modeling programs. Since the Cold War, EML has maintained the International Environmental International Environmental Sample Archive (IESA), a collection of atmospheric and other environmental samples containing isotopes present in the atmosphere during periods when nations still engaged in atmospheric testing of nuclear weapons. These samples can be used to test current samples for signs of nuclear testing and are a part of nonproliferation monitoring. The samples can also allow quantitative and qualitative standardization of monitoring instrumentation.

As part of HSMN implementation, EML scientists constructed a prototype monitoring platform on top the GSA building in New York city that is capable of detecting radiological anomalies. Radiation levels can be measured by instruments utilizing a pressurized ionization chambers (PIC), comprehensive radiation sensors (CRS), and direct analysis of trapping filters via high-resolution gamma-ray analysis. The instruments are capable of distinguishing between natural radioactive sources and artificial or man-made sources.

EML programs include surface, air, and high altitude sampling programs, soil and sediment sampling programs, and fallout measurement programs.

EML scientists have developed particulate collection systems that utilize sodium iodide gamma detectors, and RAMSCAN, a highly portable battery-operated gamma radiation detector.

Other EML facilities include pulse ionization chambers capable of measuring radon levels, a gamma ray

analysis laboratory, and a thermoluminescent dosimeter reader facility.

#### ■ FURTHER READING:

##### ELECTRONIC:

Environmental Measurements Laboratory. National Security. <<http://www.eml.doe.gov/>> (March 16, 2003).

United States Department of Energy, Office of Science. National Laboratories and User Facilities. <[http://www.sc.doe.gov/Sub/Organization/Map/national\\_labs\\_and\\_userfacilities.htm](http://www.sc.doe.gov/Sub/Organization/Map/national_labs_and_userfacilities.htm)> (March 23, 2003).

United States Department of Homeland Security. Research & Technology. <<http://www.dhs.gov/dhspublic/display?theme=27&content=374>> (March 23, 2003).

##### SEE ALSO

*Argonne National Laboratory*  
*Brookhaven National Laboratory*  
*DOE (United States Department of Energy)*  
*Lawrence Berkeley National Laboratory*  
*Lawrence Livermore National Laboratory (LLNL)*  
*Los Alamos National Laboratory*  
*NNSA (United States National Nuclear Security Administration)*  
*Oak Ridge National Laboratory (ORNL)*  
*Pacific Northwest National Laboratory*  
*Plum Island Animal Disease Center*  
*Sandia National Laboratories*

## EPA (Environmental Protection Agency)

#### ■ ROBERT G. BEST

The Environmental Protection Agency (EPA) was founded for the specific purpose of protecting human health and safeguarding the natural environment. Until the establishment of the EPA in 1970, there were no federal agencies or programs designed to deal with environmental pollution in the United States in a coordinated fashion. The EPA was assigned the unenviable task of reversing pollution that resulted from many years of unregulated environmental practices that preceded the establishment of the EPA.

Even before its inception as an agency within the federal government, it was recognized that no single entity could govern all practices and activities that had significant potential impact on the environment. Thus, the EPA was designed as an interactive agency providing direction, oversight, and assistance to many other agencies and groups whose activities bear directly and indirectly on the quality of the air, water, and land.

The EPA provides advice to the president of the United States on matters of environmental policy, and is charged with the responsibility of establishing and enforcing laws

and regulations to control the quality of the environment. The chief officer of the EPA is the administrator who is appointed by the president. EPA employs 18,000 people and operates 17 laboratories across the United States. The country is divided into ten regions, each with its own regional EPA office. The total annual budget for the EPA is nearly \$8 billion.

The EPA plays a leadership role in various aspects of environmental science including research, education and environmental evaluation and assessment. EPA works closely with other federal, state and local agencies as well as Native American tribal governments to develop environmental programs and regulations and to enforce existing laws pertaining to air, water, and land quality and purity. There are also a number of voluntary programs administered by the EPA that go beyond laws and regulations to encourage individuals and organizations to prevent pollution and conserve energy.

Research in environmental science is conducted directly by laboratories within the EPA. In addition, EPA serves as a funding source and planning resource for state governments and researchers outside of the agency. Over \$1 billion from the overall EPA budget goes to categorical grants to state and local governments. Grants are also made for the purposes of enforcement, response preparedness, information exchange networks, assistance with Native American environmental issues, and counterterrorism.

Cleanup of existing toxic waste facilities remains one of the largest and most difficult tasks for the EPA. The nation's biggest and most technically complex properties affected by toxic waste are prioritized on the National Priorities List to reverse, minimize, or prevent environmental disasters related to toxic waste. These include private and federal properties many of which have been abandoned by their owners. The Superfund was created to fund these complicated and expensive cleanup activities. EPA provides outreach and educational activities for communities surrounding the toxic waste sites to raise awareness of risks, prevention and avoidance strategies, and to promote direct involvement in cleanup activities.

**EPA and the Federal Counter-Terrorism program.** The EPA supports the federal counter-terrorism program by helping state and local agencies plan for emergencies, training first responders, providing necessary resources in the event of terrorist actions, and coordinating with key federal agencies. Three offices within the EPA participate in the counter-terrorist Program: the Chemical Emergency Preparedness and Prevention Office (CEPPO), the Office of Emergency and Remedial Response (OERR), and the Office of Air and Radiation (OAR).

Following the World Trade Center terrorist attacks in September, 2001, the EPA assumed responsibility for monitoring air and water purity at ground zero, provided decontamination operations for on-site workers, monitored

key pollutants at the Staten Island landfill site, and participated in clean up of sidewalks, streets, and buildings in the surrounding area.

#### ■ FURTHER READING:

##### BOOKS:

Binns, Tristan Boyer. *The Environmental Protection Agency*. Woburn, MA: Heineman Publishers, 2002.

##### ELECTRONIC:

United States Environmental Protection Agency. "EPA's Role and Authority in Counter Terrorism" Chemical Emergency Preparedness and Prevention <<http://yosemite.epa.gov/oswer/ceppoweb.nsf/content/ct-epro.htm#epa>> (February 15, 2003).

———. "Protecting Human Health, Safeguarding the Natural Environment" Home Page <<http://www.epa.gov/>> (February 15, 2003).

##### SEE ALSO

*Air and Water Purification, Security Issues*  
*Chemical Warfare*  
*Emergency Response Teams*  
*Environmental Issues Impact on Security*  
*FEMA (United States Federal Emergency Management Agency)*  
*Radiological Emergency Response Plan, United States Federal*  
*September 11 Terrorist Attacks on the United States*  
*Toxicology*  
*Toxins*  
*Water Supply: Counter-Terrorism*

## Epidemiology

■ ANTONIO FARINA/BRIAN D. HOYLE

Epidemiology is the study of the various factors that influence the occurrence, distribution, prevention, and control of disease, injury, and other health-related events in a defined human population. By the application of various analytical techniques including mathematical analysis of the data, the probable cause of an infectious outbreak can be pinpointed. This connection between epidemiology and infection makes microorganisms an important facet of epidemiology, and gives epidemiologists a vital link in emergency planning for public health response to a biological attack.

Molecular epidemiology has been used to trace the cause of bacterial, viral, and parasitic diseases. This knowledge is valuable in developing a strategy to prevent further outbreaks of the microbial illness, since the probable source of a disease can be identified.

Furthermore, in the era of biological weapons use by individuals, organizations, and governments, epidemiological studies of the effect of exposure to infectious microbes has become more urgently important. Knowledge of the effect of a bioweapon on the battlefield may not extend to the civilian population that might also be secondarily affected by the weapons. Thus, epidemiology is an important tool in identifying and tracing the course of an infection.

**Molecular and genetic basis of epidemiology.** Genetic epidemiology studies could result in data that would enable forensic investigators to rapidly identify bioterrorism or biological warfare agents specifically engineered or vectored to affect certain subgroups within a larger population.

Molecular epidemiology arises from varied scientific disciplines, including genetics, epidemiology and statistics. The strategies involved in genetic epidemiology encompass population studies and family studies. Sophisticated mathematical tools are now involved, and computer technology is playing a predominant role in the development of the discipline. Multidisciplinary collaboration is crucial to understanding the role of genetic and environmental factors in disease processes.

Much information can come from molecular epidemiology even if the exact genetic cause of the malady is not known. For example, the identification of a malady in generations of related people can trace the genetic characteristic, and even help identify the original source of the trait. This approach is commonly referred to as genetic screening. The knowledge of why a particular malady appears in certain people, or why such people are more prone to a microbial infection than other members of the population, can reveal much about the nature of the disease in the absence of the actual gene whose defect causes the disease.

Differences in response to pathogens is often a complex interplay of various environmental and genetic factors that require sophisticated analytical tools and techniques to identify. Aided by advances in computer technology, scientists develop complex mathematical formulas for the analysis of epidemiological models, the description of the transmission of the disease, and genetic-environmental interactions. Sophisticated mathematical techniques are now used for assessing classification, diagnosis, prognosis and treatment of many diseases.

Population studies provide data that greatly impact public health programs and emergency responses. By means of several statistical tools, genetic epidemiologic studies evaluate risk factors, inheritance and possible models of inheritance. Different kinds of studies are based upon the number of people who participate and the method of sample collection (i.e., at the time of an outbreak or after an outbreak has occurred). A challenge for the investigator is to achieve a result able to be applied with as low a bias

as possible to the general population. In other words, the goal of an epidemiological study of an infectious outbreak is to make the results from a few individuals applicable to the whole population.

A fundamental underpinning of infectious epidemiology is the confirmation that a disease outbreak has occurred. Once this is done, the disease is followed with time. The pattern of appearance of cases of the disease can be tracked by developing what is known as an epidemic curve. This information is vital in distinguishing a natural outbreak from a deliberate and hostile act, for example. In a natural outbreak the number of cases increases over time to a peak, after which the cases subside as immunity develops in the population. A deliberate release of organisms will be evident as a sudden appearance of a large number of cases at the same time.

**Tracking diseases with technology.** Many illnesses of epidemiological concern are caused by microorganisms. Examples include hemorrhagic fevers such as that caused by the Ebola virus. The determination of the nature of illness outbreaks due to these and other microorganisms involve microbiological and immunological techniques.

Various routes can spread infections (i.e., contact, air borne, insect borne, food and water intake, etc.). Likewise, the route of entry of an infectious microbe can also vary from microbe to microbe.

If an outbreak is recognized early enough, samples of the suspected cause as well as samples from the afflicted (i.e., sputum, feces) can be gathered for analysis. The analysis will depend on the symptoms. For example, in the case of a food poisoning, symptoms such as the rapid development of cramping, nausea with vomiting, and diarrhea after eating a hamburger would be grounds to consider *Escherichia coli* O157:H7 as the culprit. Analyses would likely include the examination for other known microbes associated with food poisoning (i.e., *Salmonella*) in order to save time in identifying the organism.

Analysis can involve the use of conventional laboratory techniques (e.g., use of nonselective and selective growth media to detect bacteria). As well, more recent technological innovations can be employed. An example is the use of antibodies to a known microorganism that are complexed with a fluorescent particle. The binding of the antibody to the microbes can be detected by the examination of a sample using fluorescence microscopy or flow cytometry. Molecular techniques such as the polymerase chain reaction are employed to detect genetic material from a target organism. However, the expense of the techniques such as PCR tends to limit its use to more of a confirmatory role, rather than as an initial tool of an investigation. A considerable research effort is ongoing at U.S. National Laboratories to develop quicker, less expensive, and more portable PCR equipment that can be used by inspectors and investigators.

Another epidemiological tool is the determination of the antibiotic susceptibility and resistance of bacteria.

Such laboratory techniques can be combined with other techniques to provide information related to the spread of an outbreak. For example, microbiological data can be combined with geographic information systems (GIS). GIS information has helped pinpoint the source of outbreaks. In addition to geographic based information, epidemiologists will use information including the weather on the days preceding an outbreak, mass transit travel schedules and schedules of mass-participation events that occurred around the time of an outbreak to try and establish a pattern of movement or behavior to those who have been affected by the outbreak. Use of credit cards and bank debit cards can also help piece together the movements of those who subsequently became infected.

Reconstructing the movements of people is especially important when the outbreak is an infectious disease. The occurrence of the disease over time can yield information as to the source of an outbreak. For example, the appearance of a few cases at first with the number of cases increasing over time to a peak is indicative of a natural outbreak. The number of cases usually begins to subside as the population develops immunity to the infection (e.g., influenza). However, if a large number of cases occur in the same area at the same time, the source of the infection might not be natural. Examples include a food poisoning or a bioterrorist action.

Epidemiologists were among the first scientists to effectively utilize the Internet and email capabilities to effectively communicate regarding disease outbreaks. The International Society for Infectious Diseases sponsors PROMED, the global email based electronic reporting system for outbreaks of emerging infectious diseases and toxins, is open to all sources.

#### ■ FURTHER READING:

##### BOOKS:

Trestrail, John H. *Forensic Epidemiology*. Loue, Sana, 1999.

##### PERIODICALS:

Epidemiology Program Office, CDC. "CDC's 50th Anniversary: History of CDC." *Morbidity and Mortality Weekly Report* no. 45 (1996): 525–30.

##### ELECTRONIC:

Centers for Disease Control and Prevention. "About CDC." November 2, 2002. <<http://www.cdc.gov/aboutcdc.htm>> (28 December 2002).

International Society for Infectious Diseases. ProMED-mail. May, 2003. <<http://www.promedmail.org/pls/askus/f?p=2400:1000>> (May 12, 2003).

##### SEE ALSO

*Biological Weapons, Genetic Identification*  
*Bioshield Project*  
*Bioterrorism, Protective Measures*

*CDC (United States Centers for Disease Control and Prevention)*  
*Communicable Diseases, Isolation, and Quarantine*  
*Public Health Service (PHS), United States*  
*World Health Organization (WHO)*

## Espionage

Espionage is the use of spies, or the practice of spying, for the purpose of obtaining information about the plans, activities, capabilities, or resources of a competitor or enemy. It is closely related to intelligence, but is often distinguished from it by virtue of the clandestine, aggressive, and dangerous nature of the espionage trade.

The term *espionage* comes from a French word meaning *to spy*. The Middle French *espionner* appears to be related to the Old Italian *spione*, which in turn is linguistically akin to the Old High German *spehon*. This is interesting philologically, since French, Italian, and German have very different historic roots: the first two derived from the Latin of the Roman Empire, while the third comes from the language of the Romans' "barbarian" foes across the Rhine. It is perhaps fitting that the very etymology of *espionage* would reflect surreptitious connections.

**A brief history.** Though the word itself entered the English language from the French in 1793, at a time when the foundations of modern espionage were being laid, the concept of espionage is as old as civilization. Ancient and classical era scripts often mention spies and the use of espionage (e.g., the Bible mentions spies some 100 times) while the Greek legend of the Trojan horse suggests that covert operations and "dirty tricks" are nothing new. The roots of espionage in the East are likewise very deep: in the third century b.c., both the Mauryan empire of India and the China's Ch'in dynasty ensured control over their vast realms with the help of spy networks.

Despite this early evidence of organized spying in east Asia, espionage tended to be an ad hoc enterprise until the late eighteenth century. The reign of terror that followed the French Revolution—significantly, in 1793—marked the beginnings of the modern totalitarian police state, while the American Revolution a few years earlier saw the beginnings of a consistent interface between military operations and intelligence. Military intelligence came into its own during the American Civil War, while the late nineteenth century saw the birth of the first U.S. military intelligence organizations.

**The twentieth century and beyond.** Espionage reached a new level of maturity in World War I. Although Mata Hari may





United States attorney general for the southern district of Florida Thomas Scott shows a diagram illustrating a Cuban espionage network operating illegally in the U.S. as foreign agents of the Cuban government in 1998. AP/WIDE WORLD PHOTOS.

have been the most visible, and romantic, spy of the war, there were many others on both sides. The war also gave birth to the first true totalitarian state, in Russia, and this was followed soon afterward by the establishment of fascism in Italy. Totalitarianism spawned its own elaborate spy networks, and increased the requirements for espionage activities on the part of democracies, as evidenced by the U.S. experience with Nazi and later Soviet infiltrators on American shores.

The era that perhaps most commonly comes to mind at the mention of the word *espionage* is the Cold War, which lasted from the end of World War II to the fall of the Berlin Wall and the Soviet empire. Yet the end of Soviet communism was certainly not the end of espionage, a fact that became dramatically apparent as new U.S. enemies emerged among Islamist terrorists and their supporters.

In any case, espionage is not solely the enterprise of governments: companies have long sought to gain the advantage over competitors through the use of economic or industrial espionage. In a world increasingly dominated

by huge corporations, economic espionage is not likely to disappear. Nor is espionage only undertaken against enemies: the United States has captured, and punished, spies who passed U.S. secrets to such allies as Israel and South Korea.

#### ■ FURTHER READING:

##### BOOKS:

- Bennett, Richard M. *Espionage: An Encyclopedia of Spies and Secrets*. London: Virgin Books, 2002.
- Dulles, Allen Welsh. *The Craft of Intelligence*. New York: Harper & Row, 1963.
- Haynes, John Earl. *Venona: Decoding Soviet Espionage in America*. New Haven, CT: Yale University Press, 1999.
- Martin, David C. *Wilderness of Mirrors*. New York: Harper & Row, 1980.
- Wright, Peter. *Spycatcher: The Candid Autobiography of a Senior Intelligence Officer*. New York: Viking, 1987.

## SEE ALSO

*Civil War, Espionage and Intelligence*  
*Economic Espionage*  
*Espionage and Intelligence, Early Historical Foundations*  
*Intelligence*  
*Napoleonic Wars, Espionage During*

---

## Espionage Act of 1917

---

■ ADRIENNE WILMOTH LERNER

The Espionage Act, passed in 1917 after the United States entered the World War I, prohibited the disclosure of government and industrial information regarding national defense. The act also criminalized refusal to perform military service if conscripted.

In 1914, war began in Europe. The United States declared neutrality at the beginning of the war, attempting to avoid war in Europe and unrest within its own borders. Forging alliances was difficult not only because the United States' relatively small military at the time, but also because of its large immigrant population. In the three decades preceding World War I, several million people immigrated to America, many from various nations involved in the European conflict. Making alliances with Britain and France promised to upset scores of German and Austrian sympathizers, and vice versa. Though some elements of the population were divided on the opinion of European alliances, the government favored allegiance with Britain and France. While America maintained its neutrality until 1917, it became a major supplier of money, supplies, and munitions to British and French forces. American ships transported contraband weapons across the Atlantic and between European ports. Intelligence agents and merchant ships gathered reports on German vessels and informed the British Navy of fleet activity.

In retaliation for what was viewed as acts of war and signs of allegiance with their enemies, the German government sent saboteurs to destroy American factories, warehouses, and ships that produced or held munitions bound for the western front. Several high-profile terrorist acts, most especially the demolition of Black Tom Pier near Ellis Island, New York, helped to foster a genuine concern, and to some degree an hysteria, about the danger of spies and saboteurs. When America formally joined the Allies' fight against Germany and Austria-Hungary in 1917, the government enacted tough legislation intended to aid the war effort.

The Espionage Act was one of the first pieces of wartime legislation passed. It had overwhelming favor in the government, but was more controversial to the public, especially among political radicals opposed to war, conscription, and interference with civil liberties. The act had provisions for steep penalties, including a \$10,000 fine

and 20 years imprisonment. While the act was rarely questioned as a means of controlling enemy espionage, its broad application to silence anti-war protesters and left-wing sympathizers drew criticism. Socialist advocate Eugene V. Debs was sentenced to ten years in prison for claiming in a speech that the Espionage Act itself was unconstitutional. Over 450 conscientious objectors were jailed under the provisions of the act for refusing military service.

Congress amended the Espionage Act in 1918 with the passage of the Sedition Act. The act further extended prohibition on the expression of anti-war and unpatriotic sentiments. It imposed several penalties on those convicted of "disloyal, profane, scurrilous, or abusive language" against the government, its actions, or its symbols.

While the Espionage Act was intended as wartime legislation, it continued to be invoked following the end of the war. When the Bolshevik Revolution toppled the Russian monarchy in 1917, it sparked a widespread fear of communist revolts in other nations. The period, which lasted from 1919 to 1920, became known in America as the Red Scare. During the Red Scare, the attorney general, A. Mitchell Palmer, and his assistant, John Edgar Hoover, set up a special task force to prosecute radicals under the Espionage and Sedition Acts. Nearly 2,000 people were tried and imprisoned, but Palmer's increasing zeal for his cause began to draw criticism in 1920. Palmer claimed that communist agents had infiltrated American organizations and were planning to overthrow the government on May 1, 1920. When his predicted revolution failed to materialize, many turned away from his cause. Palmer and Hoover ordered the deportation of some people convicted during the Red Scare; however, most were simply jailed in the United States. Most of the prisoners sentenced during the Red Scare were freed in 1920.

■ FURTHER READING:

BOOKS:

Kennedy, David M. *Over Here: The First World War and American Society*. New York: Oxford University Press, 1986.

SEE ALSO

*World War I*

---

## Espionage and Intelligence, Early Historical Foundations

---

■ ADRIENNE WILMOTH LERNER

Espionage is one of the oldest, and most well documented, political and military arts. The rise of the great



Belle Boyd was a spy for the Confederacy during the American Civil War.  
©BETTMANN/CORBIS.

ancient civilizations, beginning 6,000 years ago in Mesopotamia, begat institutions and persons devoted to the security and preservation of their ruling regimes. Clandestine and covert operations garner the most intrigue, but the history of espionage is better described in terms of the evolution of its more mundane components of tradecraft. Throughout history, intelligence has been defined as the collection, culling, analysis, and dissemination of critical and strategic information. Its practice and implications, however, are widely diverse.

## Espionage in the Ancient World

Historical and literary accounts of spies and acts of espionage appear in some of world's earliest recorded histories. Egyptian hieroglyphs reveal the presence of court spies, as do papyri describing ancient Egypt's extensive military and slave trade operations. Early Egyptian pharos employed agents of espionage to ferret-out disloyal subject and to locate tribes that could be conquered and enslaved. From 1,000 B.C. onwards, Egyptian espionage operations focused on foreign intelligence about the political and military strength of rivals Greece and Rome.

Egyptian spies made significant contributions to espionage tradecraft. As the ancient civilizations of Egypt, Greece, and Rome employed literate subjects in their civil services, many spies dealt with written communications.

The use of written messages necessitated the development of codes, disguised writing, trick inks, and hidden compartments in clothing to his communications. Egyptian spies were the first to develop the extensive use of poisons, including toxins derived from plants and snakes, to carry-out assassinations or acts of sabotage.

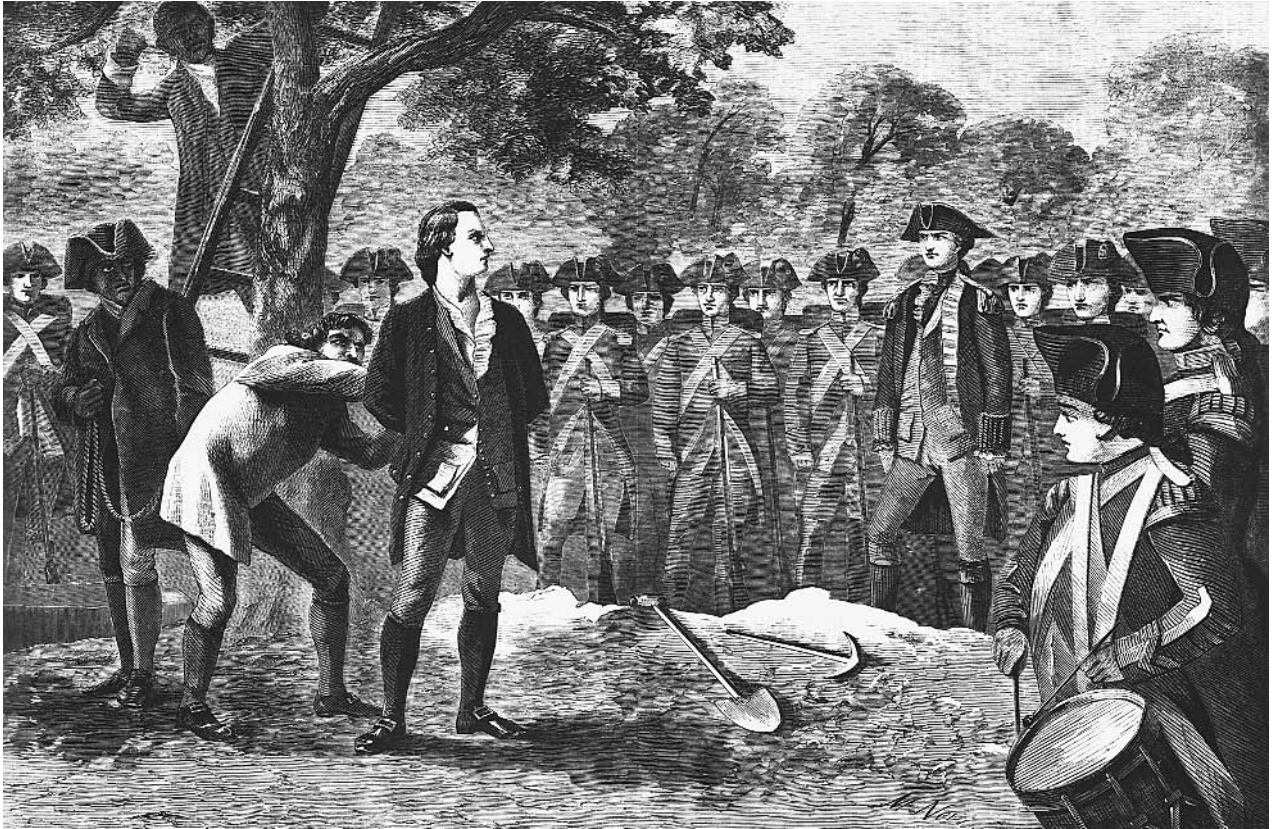
The rise of the Greek civilization brought forth new concepts of government and law enforcement. Between 1500 B.C. and 1200 B.C., Greece's many wars with its regional rivals led to the development of new military and intelligence strategies. The early Greeks relied on deception as a primary means of achieving surprise attacks on their enemies. So renowned were Greek employments of deceptive strategies, that Greek literature from antiquity celebrated its intelligence and espionage exploits. The legendary incident of the Trojan Horse, a wooden structure given to the city of Troy as gift, but which contained several hundred Greek soldiers seeking safe entrance into the heavily fortified rival city, became the symbol of Grecian intelligence prowess.

In the era of democratic Greek city-states, espionage was chiefly employed as a political tool. Agents of espionage spied on rival city-states, providing rulers with information on military strength and defenses. The most far-sighted contribution of the ancient Greek intelligence community, however, was its creation of a complex and efficient means of communication between cities. Couriers delivered messages between cities, but important messages were also relayed between a series of outposts or towers using semaphore, a form of communication that utilized signals to convey messages. Greek communications were so efficient that they remained unparalleled until the modern era.

In the Middle East, and later Byzantium, the large government bureaucracy established one of the earliest civilian intelligence agencies. Civilian agents of espionage culled information about foreign militaries and economic practices from traders, merchants, sailors, and other businessmen. Outside of the Mediterranean region, other civilizations utilized and contributed to the art of espionage. Written records from the fifth century mention the use of spies in the Indus Valley 2,500 years ago. In China, Sun Tzu penned the comprehensive military treatise, *The Art of War*, which contained several chapters devoted to the use of spies both on and off the battlefield.

No civilization in the ancient world relied more heavily on intelligence information, nor furthered the development of espionage more than ancient Rome. Over a millennium, the Romans created the largest empire of the ancient world, necessitating the governance of the most expansive infrastructure, military, and bureaucracy or the period.

Rome's most famous case of espionage and intrigue culminated in the assassination of Julius Caesar on March 15, 44 B.C. The exact details of the assassination conspiracy remain a mystery to historians, but records have established that the Roman intelligence community knew



British soldiers tie the hands of Nathan Hale (1755–1776), just before his execution for spying. ©CORBIS.

of the plot and even provided information to Caesar or his assistants providing the names of several conspirators. The information from the intelligence community was ignored.

The ever-expanding Roman Empire often spied on its neighbors. Not only did intelligence forces provide comprehensive reports on the military strength and resources of those outside the empire, but the Roman military also employed intelligence forces to infiltrate tribal organizations and convince leaders to join in alliance with Rome. If populations were judged hostile by informants, the military was informed, and engaged the opposing forces. This type of intelligence campaign was very successful in the Italian Peninsula during the fourth century B.C., but far less effective in the later campaigns to conquer North Africa and Northern Europe.

The Roman Empire possessed a fondness for the practice of political espionage. Spies engaged in both foreign and domestic political operations, gauging the political climate of the Empire and surrounding lands by eavesdropping in the Forum or in public market spaces. Several ancient accounts, especially those of the A.D. first century, mention the presence of a secret police force, the *frumentarii*. By the third century, Roman authors noted the pervasiveness and excessive censorship of the secret police forces, likening them to an authoritative force or an

occupational army. Political espionage was not limited to the more contentious parts of the Roman periphery, but was also practiced in Rome itself by rival factions of the government. Some ministries even employed saboteurs. Concern about government rivalries necessitated the creation of the *agentes in rebus*, the first exclusive counter-intelligence force.

## The Middle Ages

After the collapse of the Roman Empire in Europe, espionage and intelligence activities were confined to wartime or local service. Warring factions under barbarian lords may have used strategic espionage to gauge the strength of their opposition or learn about enemy defenses, but no written records of such activities survive. The only considerable political force in Europe during the Dark Ages was the Catholic Church, but operations on the European periphery were confined to monastic outposts that struggled for survival.

In the Middle Ages, the birth of large nation-states, such as France and England, in the ninth and tenth centuries facilitated the need for intelligence in a diplomatic setting. Systems of couriers, translators, and royal messengers carried diplomatic messages between monarchs or feudal lords. Literacy was a rarity, even in the early royal

courts, so messages were carefully delivered verbatim by couriers, or clergy acted as scribes.

Espionage remained mostly limited to battlefield operations, but the development of the feudal system, in which lords swore fealty to monarchs, created a complicated allegiance network. The web of allegiances gave rise to laws prohibiting treason, double allegiances, and political espionage against allied lords.

In the eleventh century, the Catholic Church rose to the fore in European politics. With a large bureaucratic network, the resources of feudal military forces, and the largest treasury in the world, the Church formed policy that governed all of Europe. Throughout the course of the Middle Ages, two events, the Crusades and the Inquisition, solidified the power of the Church and created the only long-standing, medieval intelligence community.

In 1095, Pope Urban II called for the first Crusade, a military campaign to recapture Jerusalem and the Holy Lands from Muslim and Byzantine rule. The Church massed several large armies, and employed spies to report on defenses surrounding Constantinople and Jerusalem. Special intelligence agents also infiltrated prisons to free captured crusaders, or sabotage rival palaces, mosques, and military defenses. The Crusades continued for nearly four centuries, draining the military and intelligence resources of most of the European monarchs.

The Crusades also changed the tenor of espionage and intelligence work within Europe itself. Religious fervor, and the desire for political consolidation, prompted thirteenth century church councils to establish laws regarding the prosecution of heretics and anti-clerical political leaders. The ensuing movement became known as the Inquisition. Although the Church used its political force as impetus for the Inquisition, enforcement of religious edicts and prosecution of violators fell to local clergy and secular authorities. For this reason, the Inquisition took many forms throughout Europe. The same movement that was terror-filled and brutal in Spain, had little impact in England and Scandinavia.

Espionage was an essential component of the Inquisition. The Church relied on vast networks of informants to find and denounce suspected heretics and political dissidents. By the early fourteenth century, Rome and the Spanish monarchs both employed sizable secret police forces to carry out mass trials and public executions. In southern France, heretical groups relied on intelligence gathered from their own resistance networks to gauge the surrounding political climate, and assist in hiding refugees.

In 1542, the process of Inquisition was centralized within the Church. Pope Paul III established the Congregation of the Holy Office, a permanent council, composed of cardinals and other officials, whose mission was to maintain the political integrity of Church. The council relied on censure and excommunication to coerce problematic individuals, forsaking the brutal cloak and dagger methods of early Inquisitors. The council maintained spies and

informants, but shifted their focus to scrutinizing the actions of Europe's monarchs and prominent aristocrats. The advent of the Renaissance in Italy in the mid-fifteenth century quelled much of the fervor and political fear that drove the Inquisition, and the movement faded.

## The Renaissance

The Renaissance marked the eclipse of the Church dominated world. Europe transitioned to more localized, nationalistic models of government, with each nation or city-state employing its own intelligence force. As nations and city-states became wealthier and gained more power, espionage enjoyed a resurgence. Competition for dominance over trade and exploration of the New World changed the political climate of Europe, and forced regimes to adopt increasingly deft measures of protecting political, military, and economic interests.

In response to the changing world, Niccolo Machiavelli, a Florentine political philosopher, published a series of books detailing the qualities and actions of effective rulers. In his works, *The Prince*, and *The Art of War*, Machiavelli advocated that rulers routinely employ espionage tradecraft, engaging in deception and spying to insure protection of their power and interests. His advice, much of which was culled from rediscovered works of Aristotle and Cicero, was intended for the ruling Medici princes of Florence. However, the works gained popularity several centuries after their 1520 publication.

In the late 1500s, the English royal court developed the premier Renaissance era spy network. Religious reforms and a schism with the Catholic Church under the rule of Henry VIII, prompted the creation of a large secret police force, commanded by the military, to locate and infiltrate Catholic loyalist cells that threatened the English monarchy. When his daughter, Elizabeth I, ascended to the throne, political tensions threatened her reign. Elizabeth chose to rebuild the flagging military to rebuff opposition from disloyal lords and their forces, but especially lobbied for the expansion of the Navy and intelligence services. The new navy dispatched foreign threats, defeating the Spanish Armada in 1558, while the intelligence services dispatched several conspiracy plots that threatened to topple Elizabeth I's reign.

The Elizabethan court gained a reputation for the ruthlessness of its spies, several of whom double and triple crossed those with whom they dealt. The Elizabethan espionage system was highly effective, but its novel contribution to the development of espionage lay in its employment practices. Instead of relying on haphazard, ill-trained volunteers, or military men, the Elizabethan intelligence community employed linguists, scholars, authors, engineers, and scientists, relying on professional experts to seek and analyze intelligence information.

Technological development in the Renaissance altered the practice of espionage. The development of small

firearms, such the pistol, aided cloak and dagger operations. Chemists invested invisible inks, and the rebirth of complex mathematics revived encryption and code methods long dormant since Antiquity. Telescopes, magnifying glasses, the camera obscura, and clocks facilitated the remote surveillance and the effective use of “dead drops” to pass information between agents. Travel became easier, but that ease soon prompted territorial growth and the rebirth of vast empires.

## The Birth of Modern Espionage: The Age of Empires, Industrial Revolution, and the Nineteenth Century

Espionage in the Age of Empires, a period that spanned from 1700 to almost 1900, saw its greatest development in the numerous conflicts and wars that occurred in Europe, and between rival colonial powers in Europe and abroad. Industrialization, economic and territorial expansion, the diversification of political philosophies and regimes, and immigration all transformed the world’s intelligence communities.

During the French Revolution, in the 1790s, all factions relied heavily on espionage. However, the period marked by the dictatorship of Robespierre is most infamous. Informant networks denounced traitors to the new republic, and tracked down refugee aristocrats and clergy for trial and execution. The wide application of treason laws and charges marked one of the greatest abuses of intelligence powers in the modern era.

The American Revolution (1776–1783), and colonial wars for independence in South America in the 1820s and 1830s, marked the end of Europe’s New World empires. European nations turned their attention to Africa and the Orient. The ensuing land grab inflamed tensions among European nations, changing the balance of European power and creating a complicated alliance system. Colonial rulers employed secret police and agents of espionage throughout their territorial holdings, hoping to quell anti-colonial rebellions and separatist movements.

Imperialism not only changed the world political balance, but transformed economics. Modern industrial espionage was born in the pan-European revolutions of 1848. The series of regional conflicts pitted workers against landed gentry, liberals against conservatives, and monarchists against republicans, communists, and other political groups. Many governments, especially those of England, France, and Prussia, employed spies to infiltrate political and labor organizations and report on any anti-government activities. Labor organizations often spied on each other, reporting on working conditions, factory operations, mining productivity, and other concerns. Many

radical workers’ organizations carried out acts of sabotage, destroying factories, mines, and government property. After armed conflict abated, many governments continued to conduct surveillance on dissident and workers’ groups, within a decade, the same principals of industrial espionage were increasingly employed against foreign economic interests.

Industrialization revolutionized tradecraft with the proliferations of gadgets for the concealment, transcription, and analysis of intelligence information. The invention of dynamite aided saboteurs. Advances in chemistry and chemical production transformed everything from dyes and inks, to poisons and acids. Chemical weapons and poison gasses were developed during this time, but were considered too inhumane for strategic use until World War I. The discipline of forensic science added scientific methodology to the investigation of crimes and the analysis of intelligence information.

The collection of intelligence information forever changed in 1837, with the invention of the daguerreotype, the first practical form of photography. Though not able to be widely incorporated into intelligence practices until the 1860s, the photograph permitted agents of espionage to portray targets, documents, and other interests as they actually were. As soon as photo development became more practical with the advent of film, in lieu of glass plates, cameras were made smaller, disguised, or placed in mundane items for use in espionage. Until the advent of electronic data storage in the twentieth century, the photograph was the best means of copying and transmitting information.

Improvements in transportation and communications also transformed espionage operations. On May 24, 1844, Samuel Morse, sent the first message via telegraph. His code (Morse code) and the telegraph were able to send messages over lines in a matter of minutes, requiring only knowledge of the operational code. As soon as governments began to use telegraphs to send vital communications, rival intelligence services learned to tap the line, gaining access to secret communications and conducting detailed surveillance from a comfortable distance. Use of the telegraph necessitated the development of complex codes, and the creation of specialized cryptology departments. By the turn of the twentieth century, most national intelligence operations in Europe and the United States involved communications surveillance and the tapping of both wired, and wireless, telegraphs.

Just as the discovery of the New World, and the development of fast ships in the seventeenth century altered the scope of espionage, so to did the invention of the locomotive and the proliferation of railroads. Railroads also became primary targets of enemy sabotage, and one of the main protective objectives of counterintelligence personnel. Ease of travel facilitated communications and surveillance, permitting agents to travel to foreign destinations under the guise of tourists without arousing suspicion. Movement, travel, and immigration during the nineteenth century provided many nations,

especially the United States, with a field of language and culture experts.

By the dawn of the twentieth century, espionage had evolved into a highly specialized, technical field. Far from the battlefield and political intrigue of the ancient world, modern espionage involves more research and analysis than field operations. Specialized military units are still used for strategic intelligence gathering, but most nations have developed large, centralized, civilian intelligence communities that conduct operations in wartime and peacetime with increasing technological sophistication.

#### ■ FURTHER READING:

##### BOOKS:

Boardman, John, Jasper Griffen, and Oswyn Murray. *Oxford History of the Classical World*. New York: Oxford University Press, 1986.

Holmes, George. *Oxford History of Medieval Europe*. New York: Oxford University Press, 1988.

##### SEE ALSO

*Cryptology, History  
Napoleonic Wars, Espionage During  
Revolutionary War, Espionage and Intelligence  
War of 1812*

## Estonia, Intelligence and Security

Estonia maintains one central intelligence and security agency, the *Kaitsepolitseiamet* (KPol), Security Police Board. The KPol administers intelligence gathering and information analysis, and reports its findings to the executive branch of the government. KPol governs several operational divisions, including Counterintelligence, the Security Police, the Anti-terrorism Bureau, Constitutional Protection Bureau, and Anti-Corruption Bureau. The KPol's main objective is the protection of national interests and national sovereignty. The agency seeks both domestic and foreign intelligence.

Estonia emerged as a modern, independent nation in 1920. During World War II, however, the nation was invaded by both Soviet and German forces. After the war, Estonia fell in the Soviet sphere of influence. Estonia lost its sovereignty, becoming part of the Soviet Union for four decades. In 1988, the Estonian parliament decreed the nation autonomous, but Soviet forces kept the nation from seceding for over a year. After the fall of the Berlin Wall and the Iron Curtain in 1989, Estonia began the process of

regaining its status as an independent nation. The collapse of the Soviet Union in 1991 allowed Estonia to finally reemerge as a democratic, independent nation.

The move to democracy in Estonia required extensive social, economic, and government reform. The new Estonian government sought to dissolve any remaining Soviet institutions, most especially those that were used as state-sponsored instruments of suppression, intended to quell nationalism. Estonia did not maintain its own intelligence community under Soviet rule, but had to distance its new, national intelligence agencies from the legacy of the KGB and Soviet secret police.

Corruption is a primary concern for the Estonia government. A legacy of Soviet occupation, government corruption was prevalent in the early 1990s. However, anti-crime and corruption task forces, as well as intelligence surveillance of government officials, has greatly reduced the problem. Business corruption, as well as incursions into the national economy by the Russian mafia, are also targeted by KPol intelligence operations.

Today, Estonia is actively pursuing membership in several international organizations. Reforms have aided a rapid transformation of the Estonian economy. Diplomatically, Estonia gravitates toward Europe, but maintains ties with neighboring Russia.

##### SEE ALSO

*Cold War (1945–1950), The Start of the Atomic Age  
Cold War (1950–1972)  
Cold War (1972–1989): The Collapse of the Soviet Union  
European Union*

## European Union

#### ■ ADRIENNE WILMOTH LERNER

The European Union (EU) is a long-standing political and economic federation of autonomous European nations. With the consent of member states, the EU legislates a variety of issues by treaty, including trade, customs, travel, currency, and defense. Members choose to participate in various EU institutions, delegating sovereignty in order to achieve common goals.

The organization embraces democracy and the rule of law, requiring member states to possess some form of representative government, elected by universal adult suffrage of the adult citizenry. The mission of the EU is to promote economic growth in Europe, create a strong international market, lobby for European interests in the international community, raise standards of living, and promote peace.

**History.** European integration, the process that eventually yielded the EU, began on May 9, 1950, when France

proposed to create a European trade organization. Two years later, France and Germany established the European Coal and Steel Community. Both nations sought to solve disputes over coal mining territories and industry competition unresolved since the end of the Second World War. Belgium later joined France and Germany, uniting most of Western Europe's continental coal and steel industry.

Continued success of the European Coal and Steel Community prompted its president to lobby European governments for the establishment of a large-scale economic and trade union. In 1957, six nations (France, Germany, Belgium, the Netherlands, Luxembourg, and Italy) signed the Treaty of Rome, establishing the European Economic Community (EEC). The EEC standardized some tariffs, opened borders to free trade, promoted industry cooperation, regulated industry standards, and synchronized export practices.

In 1967, the member nations brought the European Coal and Steel Community and the European Atomic Energy Community (Euratom) into the fold of the EEC. The new unified organization was officially named the European Community (EC), though many continued to use the older designation, EEC, to refer to the new union.

Several nations in Europe chose not to join the original EEC, the most prominent of which was Great Britain. In January 1960, Britain formed a more loosely regulated economic union to rival the EC. The European Free Trade Association (EFTA), known colloquially as the "Seven," included Britain, Austria, Denmark, Norway, Portugal, Sweden, and Switzerland. A year later, Britain applied for membership in the EC, but France rejected their proposal to join the organization. The French government subsequently vetoed Britain's second application for membership in 1964.

Britain, along with Ireland, Denmark, and Norway, became members of the EC in 1973. In a series of accessions, six more nations joined the EC before 1995. The organization adopted a more ambitious mandate in the 1990s, establishing government and judiciary organizations in an attempt to closely unite European interests. Adoption of the new mandate by member states established the European Union.

**Organization.** Today's EU mission encompasses more than economic goals. The principal objectives of the EU are to establish European citizenship, ensure civil rights of European citizens, promote social progress, protect European security, and ensure justice. To these ends, the European Union maintains its own government and supporting agencies. These institutions are granted sovereignty by the member states to legislate European affairs and create international law. Final adoption of EU policy, however, is left to the individual member states.

Five primary institutions comprise the government of the EU. Its overall structure embraces the three-branch

democratic model of government, with executive, legislative, and judicial bodies. The European Commission is the primary institution of the executive branch. Members are elected or appointed by the European Parliament. The Council of the Union is composed of representatives from the governments of the member states. The Council governs the EU as a collective, requiring majority support to set or endorse policy.

The European Parliament, the legislative body, is elected by the people of the member states. Committees within the European Parliament address specific concerns, such as health care, preservation of the environment, and trade regulation. The Court of Auditors, the committee responsible for overseeing and managing the EU budget, remains separate from every branch of the EU government, but works closely with the Parliament to appropriately allocate funds and resources.

The EU judiciary is the Court of Justice. The jurisdiction of the European court is somewhat dubious, and member states recognize its authority to varying degrees. The court is similar in structure and function to those of the United Nations, but is permitted to pursue only cases that affect member states.

A myriad of committees and support institutions comprise the rest of the EU government. The EU maintains its own central finance system, including the European Central Bank and the European Investment Bank. These contain funds used by the EU or granted to individual member states for various joint projects. In 1999, nine nations adopted a standard European currency, the Euro.

**Membership.** Fifteen member states currently comprise the European Union: Austria, Belgium, Denmark, Germany, Greece, Finland, France, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden, and the United Kingdom of Great Britain and Northern Ireland. These member nations participate in the EU to varying degrees. For example, Britain participates in EU economic and trade associations, but uses its national currency, the pound, instead of the euro.

In 1998, the EU began negotiations with several eastern and southern European nations regarding EU expansion. Still recovering from decades of Soviet Communist domination, many of these nations possess fledgling free market economies. Introduction of former Eastern Block nations into the EU holds the potential for economic growth and expanded investment opportunities for European industry. However, expansion also poses liabilities to more economically robust EU nations.

The EU granted admission to the following candidate nations in 2002: Czech Republic, Cyprus, Estonia, Hungary, Latvia, Lithuania, Malta, Poland, Slovenia, and Slovakia. These nations officially join the EU on May 1, 2004, assuming that they ratify membership in a national, public referendum. Bulgaria and Romania are scheduled to join the EU in 2007.



Some negotiations on expansion proved contentious. The EU denied Turkey's application to join the organization, despite the nation's numerous economic and trade associations with Europe. The EU will review Turkey's application again in 2004, if the nation furnishes evidence that it has met EU demands to improve human rights and maintain a stable democratic government. The nation of Cyprus, divided between Grecian southern Cyprus and nationalist Turkish Cypriots, failed to reunify before the EU accepted the national proposal to join the EU. Therefore, only the independent half of the nation will join the EU in 2004.

Some nations in Western Europe have chosen to remain outside of the European Union. Switzerland, and EFTA members, did not join the union on the grounds that membership in the EU threatened its national policy of declared neutrality. Norway also chose to exclude itself from EU membership.

**Common defense and security: the future of the EU.** A series of treaties in the 1980s and 1990s expanded the political, defense, and military role of the European Union. Formerly an instrument of economic and social policy, the EU adopted the Common Foreign and Security Policy (CFSP) in response to global instability and the rise of terrorism. The creation of the European Security and Defense Policy (ESDP) followed, outlining the EU's international responsibilities to defend European territory and interests while cooperating with organizations such as the North Atlantic Treaty Organization (NATO) and the United Nations.

Defense and security strategy remains one of the most contentious aspects of European Union policy. Some member states prefer to rely on their connections to NATO, or their own defenses, for protection. Others are wary of creating an EU military force under international command.

The EU established several crisis management tasks, known as the Petersberg Tasks, a foreign policy priority. For the purpose of humanitarian aid and rescue, peacekeeping, and crisis management, the EU created a military task force of 60,000 reserve troops. Member states can choose to contribute and deploy national military troops to EU operations on a case-by-case basis.

The EDSP launched its first operation, a police mission in Bosnia and Herzegovina, in January 2003. The first EU military operation commenced in Macedonia two months later.

With the aid of ESDP liaisons in 2002, the EU candidate nations signed a declaration warning Iraqi leader Saddam Hussein that military action was justified if United Nations weapons inspections were not permitted to freely proceed. The statement angered several EU members, causing a rift in EU foreign policy. Although the EU did not formally support the subsequent United States led action in Iraq, several member and candidate nations supported the Coalition military action. Some of the most influential

EU nations, such as France and Germany, voiced strong opposition to the 2003 war in Iraq.

#### ■ FURTHER READING :

#### ELECTRONIC:

European Union. <<http://www.europa.eu.int>> (May 9, 2003).

#### SEE ALSO

*NATO (North Atlantic Treaty Organization)*  
*United Nations Security Council*

---

## Executive Orders and Presidential Directives

---

Executive orders and presidential directives, as their name suggests, come from the president of the United States. Executive orders are unclassified, and in practice carry the force of law, though they remain controversial inasmuch as they amount to government by virtual edict. Presidential directives are classified, and thus the public is not even aware of their content. Both types of rules, along with directives from various security agencies, provide the guidelines by which the United States intelligence community operates.

**Executive orders.** President Theodore Roosevelt initiated the practice of issuing executive orders at the beginning of the twentieth century, and their numbers grew with each successive administration, until by the early twenty-first century they numbered more than 50,000. The actual numbers designating the orders are relatively low: for example, that of the order by which President George W. Bush froze terrorist organization assets in the aftermath of the September 11, 2001, attacks is only 13224. But these low numbers conceal the fact that many executive orders have been amended by number or letter extensions thus: xxxx-A, xxxx-B, and so on.

Among the executive orders of significance to the intelligence community are those dealing with classification and declassification of national security information. These go back at least to the time of President Richard M. Nixon, whose Executive Order 11652 (1972) stipulated that virtually all records would be declassified after 30 years. President Carter, in Executive Order 12065 (1978), called for a review of records after just 20 years with an eye toward declassification. In 1982, President Ronald Reagan bucked the trend, tightening the standards with Executive Order 12356, which favored continued classification and even provided conditions for the reclassification of previously declassified documents. With Executive Order 12958,

discussed elsewhere in the context of classified information, President Clinton returned to the earlier trend toward declassification.

Most administrations from the 1960s onward have also issued executive orders concerning the intelligence community, its operations, and/or specific aspects of security and intelligence. President Reagan, for instance, signed Executive Order 12333, "United States Intelligence Activities," in April 1981. President Clinton's Executive Order 12968, in 1995, provided conditions whereby security clearances would be granted.

The Supreme Court has ruled that executive orders have the force of law only if they are consistent with the provisions of the Constitution and/or receive congressional authorization. In practice, however, these orders have served as a means whereby presidents make law without recourse to the system prescribed in the Constitution.

**Presidential directives and other guidelines.** At least executive orders are unclassified; by contrast, presidential directives are not open to public knowledge. They exist, however, and have helped to guide security and intelligence policy since the administration of President John F. Kennedy.

Most administrations have their own names for presidential directives; thus under President George Bush (president, 1989–1993), they were known as national security directives (NSDs). President Clinton called them presidential decision directives, while President George W. Bush designated them national security presidential directives. An example of a known presidential directive is NSD 63, issued by George H. W. Bush in October 1991 to guide background checks for the issuance of Sensitive Compartmented Information (SCI) security clearances.

In addition to executive orders and presidential directives, other regulations guiding intelligence and security operations in the United States include National Security Council (NSC) intelligence directives (NSCIDs), Director of Central Intelligence (DCI) directives (DCIDs), and Department of Defense (DoD) directives. Whereas the guidelines from the president tend to be general, those from the NSC, DCI, and DoD are much more specific.

#### ■ FURTHER READING:

##### BOOKS:

Mayer, Kenneth R. *With the Stroke of a Pen: Executive Orders and Presidential Power*. Princeton, NJ: Princeton University Press, 2001.

*National Security: The Use of Presidential Directives to Make and Implement United States Policy: Report to the Chairman, Committee on Government Operations, House of Representatives*. Washington, D.C.: Government Printing Office, 1988.

Richelson, Jeffrey T. *The United States Intelligence Community*, third edition. Boulder, CO: Westview Press, 1995.

##### ELECTRONIC:

Executive Orders. National Archives and Records Administration. <[http://www.archives.gov/federal\\_register/executive\\_orders/executive\\_orders.html](http://www.archives.gov/federal_register/executive_orders/executive_orders.html)> (January 22, 2003).

##### SEE ALSO

*Classified Information*  
*Interagency Security Committee, United States PFIAB (President's Foreign Intelligence Advisory Board)*  
*President of the United States (Executive Command and Control of Intelligence Agencies)*  
*Security Clearance Investigations*  
*Terrorist Organizations, Freezing of Assets*

---

## Explosive Coal

---

#### ■ DAVID TULLOCH

Explosives disguised as coal were made in World War II by both the British Special Operations Executive (SOE) and the American Office of Strategic Services (OSS) to be used against such targets as steam locomotives, ships, and factory furnaces. Explosive coal allowed operatives to target relatively unguarded coal storage areas that supplied heavy security installations. Many other disguised explosives were also made.

The SOE's Section D made a number of disguised explosives. Their explosive coal design was a hollow shell in two halves that looked like coal and could be filled with plastic explosive and fitted with an igniter match, fuse, and detonator. The coal could then be hidden in enemy coal bins, and would be triggered when burned. Dead rats filled with plastic explosive were also used against the same targets. Like the coal, these could be casually tossed into coal stores by operatives, or left in factories, as the most common method of disposal of dead vermin was to burn them in the nearest furnace. After initial successes in Belgium, the Germans discovered a downed British plane containing a number of these vermin bombs, and so changed their rat disposal methods. The SOE also produced explosive logs, cow-pats, mule dung, and even explosive elephant dung.

The OSS Office of Science Research and Development went a step further with their explosive coal design by providing a Coal Camouflage Kit. Coal comes in many varieties, and there are significant differences in appearance depending on the region and grade of coal. Lignite coal, for example, is brown in color, while anthracite coal is a deep black. The Camouflage Kit contained paints, brushes, and other tools to enable operatives to match the explosive coal more exactly to the target type. Another

innovative OSS-disguised explosive looked identical to wheat flour and could even be added to milk or water and baked into a loaf before use. While having great novelty value, the actual operational value of weapons such as explosive coal was small in comparison to more conventional forms of explosives.

■ FURTHER READING:

BOOKS:

Ladd, James, and H. Keith Melton. *Clandestine Warfare: Weapons and Equipment of the SOE and OSS*. London: Blandford, 1988.

Melton, H. Keith. *OSS Special Weapons and Equipment: Spy Devices of World War Two*. New York: Sterling Publishing Co, Inc., 1991.

ELECTRONIC:

International Spy Museum, 800 F Street NW, Washington, D.C. <<http://www.spymuseum.org>.> (December 19, 2002).

Museum of World War II, 46 Eliot Street, Natick, MA, 2001. <<http://www.museumofworldwar2.com>.> (December 19, 2002).

SEE ALSO

*OSS (United States Office of Strategic Services*

E N C Y C L O P E D I A   O F  
**Espionage, Intelligence, and Security**



E N C Y C L O P E D I A O F

# Espionage, Intelligence, and Security

*This page intentionally left blank*

E N C Y C L O P E D I A O F  
Espionage, Intelligence, and Security

K. LEE LERNER AND BRENDA WILMOTH LERNER, EDITORS

v o l u m e  
1 2 1  
F - Q



THOMSON  
—★—™  
GALE



## Encyclopedia of Espionage, Intelligence, and Security

K. Lee Lerner and Brenda Wilmoth Lerner, editors

**Project Editor**  
Stephen Cusack

**Editorial**  
Erin Bealmear, Joann Cerrito, Jim Craddock,  
Miranda Ferrara, Kristin Hart, Melissa Hill,  
Carol Schwartz, Christine Tomassini, Michael  
J. Tyrkus, Peter Gareffa

**Permissions**  
Lori Hines

**Imaging and Multimedia**  
Dean Dauphinais, Leitha Etheridge-Sims, Mary  
K. Grimes, Lezlie Light, Luke Rademacher

**Product Design**  
Kate Scheible

**Manufacturing**  
Rhonda Williams

© 2004 by Gale. Gale is an imprint of The  
Gale Group, Inc., a division of Thomson  
Learning, Inc.

Gale and Design™ and Thomson Learning™  
are trademarks used herein under license.

*For more information, contact*  
The Gale Group, Inc.  
27500 Drake Rd.  
Farmington Hills, MI 48331-3535  
Or you can visit our Internet site at  
<http://www.gale.com>

### ALL RIGHTS RESERVED

No part of this work covered by the copyright  
hereon may be reproduced or used in  
any form or by any means—graphic,  
electronic, or mechanical, including  
photocopying, recording, taping, Web  
distribution, or information storage retrieval  
systems—without the written permission of  
the publisher.

For permission to use material from this  
product, submit your request via Web at  
<http://www.gale-edit.com/permissions>, or you  
may download our Permissions Request form  
and submit your request by fax or mail to:

*Permissions Department*  
The Gale Group, Inc.  
27500 Drake Rd.  
Farmington Hills, MI 48331-3535  
Permissions Hotline:  
248-699-8006 or 800-877-4253, ext. 8006  
Fax: 248-699-8074 or 800-762-4058

### Cover Photos

Volume 1: Ethel and Julius Rosenberg  
following arraignment on charges of  
espionage, August 23, 1950.  
©Bettmann/Corbis

Volume 2: SR-71 Blackbird, c. 1991. ©Corbis

Volume 3: Clean-up crews scour the American  
Media Inc. building in Boca Raton, Florida,  
after the discovery of anthrax spores, October  
9, 2001. AP/Wide World Photos.

While every effort has been made to  
ensure the reliability of the information  
presented in this publication, The Gale Group,  
Inc. does not guarantee the accuracy of  
the data contained herein. The Gale Group,  
Inc. accepts no payment for listing; and  
inclusion in the publication of any  
organization, agency, institution, publication,  
service, or individual does not imply  
endorsement of the editors or publisher.  
Errors brought to the attention of the  
publisher and verified to the satisfaction of  
the publisher will be corrected in future  
editions.

### Library of Congress Cataloging-in-Publication Data

Encyclopedia of espionage, intelligence, and security / K. Lee Lerner  
and Brenda Wilmoth Lerner, editors.  
p. cm.

Includes bibliographical references and index.

ISBN 0-7876-7546-6 (set : hardcover : alk. paper) — ISBN  
0-7876-7686-1 (v. 1) — ISBN 0-7876-7687-X (v. 2) — ISBN 0-7876-7688-8  
(v. 3)

1. Espionage—Encyclopedias. 2. Intelligence service—Encyclopedias.  
3. Security systems—Encyclopedias. I. Lerner, K. Lee. II. Lerner,  
Brenda Wilmoth.  
JF1525.I6E63 2004  
327.12'03—dc21

2003011097

This title is available as an e-book.  
ISBN 0-7876-7762-0

Contact your Gale sales representative for ordering information.

Printed in the United States of America  
10 9 8 7 6 5 4 3 2 1



# Contents

INTRODUCTION	VII
ADVISORS AND CONTRIBUTORS	XI
LIST OF ENTRIES	XIII
 The Encyclopedia of Espionage, Intelligence, and Security	 1
 GLOSSARY	 289
CHRONOLOGY	317
SOURCES	353
INDEX	403

*This page intentionally left blank*

# Introduction

In composing *The Encyclopedia of Espionage, Intelligence, and Security (EEIS)*, our goal was to shape a modern encyclopedia offering immediate value to our intended readers by emphasizing matters of espionage, intelligence, and security most frequently in the news.

*EEIS* is not intended as a classical “spy book,” filled with tales of daring operations. Instead, within a framework of historical overviews, *EEIS* emphasizes the scientific foundations, applications of technology, and organizational structure of modern espionage, intelligence, and security. High school and early undergraduate students can use this book to expand upon their developing awareness of the fundamentals of science, mathematics, and government as they begin the serious study of contemporary issues.

*EEIS* is also intended to serve more advanced readers as a valuable quick reference and as a foundation for advanced study of current events.

*EEIS* devotes an extensive number of articles to agencies and strategies involved in emerging concepts of homeland security in the United States. Faced with a daunting amount of information provided by agencies, organizations, and institutes seeking to put their best foot forward, we have attempted to allocate space to the topics comprising *EEIS* based upon their relevance to some unique facet of espionage, intelligence, or security—especially with regard to science and technology issues—as opposed to awarding space related to power of the agency or availability of material.

A fundamental understanding of science allows citizens to discern hype and disregard hysteria, especially with regard to privacy issues. Spy satellites powerful enough to read the details of license plates do so at peril of missing events a few steps away. With regard to electronic intercepts, the capability to identify what to carefully examine—often a decision driven by mathematical analysis—has become as essential as the capacity to gather the intelligence itself. Somewhere between the scrutiny of

Big Brother and the deliberately blind eye lie the shadows into which terrorists often slip.

With an emphasis on the realistic possibilities and limitations of science, we hope that *EEIS* finds a useful and unique place on the reference shelf.

It seems inevitable that within the first half of the twenty-first century, biological weapons may eclipse nuclear and chemical weapons in terms of potential threats to civilization. Because informed and reasoned public policy debates on issues of biological warfare and bioterrorism can only take place when there is a fundamental understanding of the science underpinning competing arguments, *EEIS* places special emphasis on the multifaceted influence and applications of the biological sciences and emerging biometric technologies. Future generations of effective intelligence and law enforcement officers seeking to thwart the threats posed by tyrants, terrorists, and the technologies of mass destruction might be required to be as knowledgeable in the terminology of epidemiology as they are with the tradecraft of espionage.

Knowledge is power. In a time where news can overwhelm and in fact, too easily mingle with opinion, it is our hope that *EEIS* will provide readers with greater insight to measure vulnerability and risks, and correspondingly, an increased ability to make informed judgments concerning the potential benefits and costs of espionage, intelligence, and security matters.

■ K. LEE LERNER & BRENDA WILMOTH LERNER, EDITORS  
CORNWALL, U.K.  
MAY, 2003

## How to Use the Book

The *Encyclopedia of Espionage, Intelligence, and Security* was not intended to contain a compendium of weapons systems. Although *EEIS* carries brief overviews of specifically selected systems commonly used in modern intelligence operations, readers interested in detailed information regarding weapons systems are recommended

to *Jane's Strategic Weapon Systems*, or *Jane's Defense Equipment Library*.

Although *EEIS* contains overview of significant historical periods and events, for those readers interested in additional information regarding the history of espionage operations and biographies of intelligence personnel, the editors recommend Jeffrey T. Richelson's *A Century of Spies: Intelligence in the Twentieth Century* (Oxford University Press, 1995), Vincent Buranelli and Nan Buranelli's *Spy/Counterspy: An Encyclopedia of Espionage* (New York: McGraw-Hill, 1982), and Allen Dulles', *The Craft of Intelligence* (New York: Harper & Row, 1963).

The articles in *EEIS* are meant to be understandable by anyone with a curiosity about topics in espionage, intelligence, and security matters, and this first edition of the book has been designed with ready reference in mind:

- Entries are arranged alphabetically. In an effort to facilitate easy use of this encyclopedia, and to attempt order in a chaotic universe of names and acronyms the editors have adopted a "common use" approach. Where an agency, organization, or program is known best by its acronym, the entry related to that organization will be listed by the acronym (e.g. FEMA is used instead of Federal Emergency Management Agency). To facilitate use, the editors have included a number of "jumps" or cross-referenced titles that will guide readers to desired entries.
- To avoid a log jam of terms starting with "Federal" and "United States," titles were broken to most accurately reflect the content emphasized or subject of agency authority.
- "**See Also**" references at the end of entries alert the readers to related entries not specifically mentioned in the body of the text that may provide additional or interesting resource material.
- An extensive **Glossary** of terms and acronyms is included to help the reader navigate the technical information found in *EEIS*.
- The **Chronology** includes significant events related to the content of the encyclopedia. Often accompanied by brief explanations, the most current entries date represent events that occurred just as *EEIS* went to press.
- A **Sources** section lists the most worthwhile print material and web sites we encountered in the compilation of this volume. It is there for the inspired reader who wants more information on the people and discoveries covered in this volume.
- A comprehensive general **Index** guides the reader to topics and persons mentioned in the book. Bolded page references refer the reader to the term's full entry.
- The editors and authors have attempted to explain scientific concepts clearly and simply, without sacrificing fundamental accuracy. Accordingly, an advanced understanding of physics, chemistry, or biochemistry is not assumed or required. Students and other readers should not, for example, be intimidated or deterred by the complex names of biochemical

molecules—where necessary for complete understanding, sufficient information regarding scientific terms is provided.

- To the greatest extent possible we have attempted to use Arabic names instead of their Latinized versions. Where required for clarity we have included Latinized names in parentheses after the Arabic version. Alas, we could not retain some diacritical marks (e.g. bars over vowels, dots under consonants). Because there is no generally accepted rule or consensus regarding the format of translated Arabic names, we have adopted the straightforward, and we hope sensitive, policy of using names as they are used or cited in their region of origin.
- *EEIS* relies on open source material and no classified or potentially dangerous information is included. Articles have been specifically edited to remove potential "how to" information. All articles have been prepared and reviewed by experts who were tasked with ensuring accuracy, appropriateness, and accessibility of language.
- With regard to entries regarding terrorist organizations, *EEIS* faced a serious dilemma. For obvious reasons, it was difficult to obtain balanced, impartial, and independently verifiable information regarding these organizations, nor could *EEIS* swell to incorporate lengthy scholarly analysis and counter-analysis of these organizations without losing focus on science and technology issues. As a compromise intended to serve students and readers seeking initial reference materials related to organizations often in the news, *EEIS* incorporates a series of supplemental articles to convey the information contained in the U.S. Department of State annual report to Congress titled, *Patterns of Global Terrorism*, 2001. These articles contain the language, assertions of fact, and views of the U.S. Department of State. Readers are encouraged to seek additional information from current U.S. Department of State resources and independent non-governmental scholarly publications that deal with the myriad of issues surrounding the nature and activities of alleged terrorist organizations. A number of governmental and non-governmental publications that deal with these issues are cited in the bibliographic sources section located near the index.

Key *EEIS* articles are signed by their authors. Brief entries were compiled by experienced researchers and reviewed by experts. In the spirit of numerous independent scientific watchdog groups, during the preparation of *EEIS* no contributors held a declared affiliation with any intelligence or security organization. This editorial policy not only allowed a positive vetting of contributors, but also assured an independence of perspective and an emphasis on the fundamentals of science as opposed to unconfirmable "insider" information.

When the only verifiable or attributable source of information for an entry comes from documents or information provided by a governmental organization (e.g., the U.S. Department of State), the editors endeavored to carefully note when the language used and perspective offered was that of the governmental organization.

Although some research contributors requested anonymity, no pseudonyms are used herein.

## Acknowledgments

The editors wish to thank Herbert Romerstein, former USIA Soviet Disinformation Officer and Coordinator of Programs to Counter Soviet Active Measures, United States Information Agency, for his assistance in compiling selected articles.

The editors wish to thank Lee Wilmoth Lerner for his assistance in compiling technical engineering data for inclusion in *EEIS*.

The editors acknowledge the assistance of the members of the Federation of American Scientists for the provision of reports and materials used in the preparation of selected articles.

Although certainly not on the scale of the challenge to provide security for a nation with approximately 85 deep-draft ports, 600,000 bridges, 55,000 independent water treatment systems, 100 nuclear power plants, and countless miles of tunnels, pipelines, and electrical and communications infrastructure, the task of incorporating changes brought on by creation of the Department of Homeland Security—and the most massive reorganization of the United States government since World War II—as this book went to press provided a unique challenge to *EEIS*

writers and advisors. The editors appreciate their dedication and willingness to scrap copy, roll up their sleeves, and tackle anew the smorgasbord of name and terminology changes.

As publishing deadlines loomed, *EEIS* was also well served by a research staff dedicated to incorporating the latest relevant events—especially information related to the search for weapons of mass destruction—that took place during war in Iraq in March and April of 2003.

*EEIS* advisors, researchers, and writers tenaciously attempted to incorporate the most current information available as *EEIS* went to press. The editors pass any credit or marks for success in that effort, and reserve for themselves full responsibility for omissions.

The editors gratefully acknowledge the assistance of many at St. James Press for their help in preparing *The Encyclopedia of Espionage, Intelligence, and Security*. The editors extend thanks to Mr. Peter Gareffa and Ms. Meggin Condino for their faith in this project. Most directly, the editors wish to acknowledge and thank the project editor, Mr. Stephen Cusack, for his talented oversight and for his tireless quest for secure engaging pictures for *EEIS*.

The editors lovingly dedicate this book to the memory of Wallace Schaffer, Jr., HM3, USNR, who died on January 8, 1968, in Thua Thien (Hue) Province, Vietnam.

“A small rock holds back a great wave.”—Homer, *The Odyssey*.

*This page intentionally left blank*

## Advisors and Contributors

**Julie Berwald, Ph.D.**

*Geophysicist, writer on marine science, environmental biology, and issues in geophysics.*  
Austin, Texas

**Robert G. Best, Ph.D.**

*Clinical cytogeneticist and medical geneticist who has written on a range of bioscience issues*  
Director, Division of Genetics  
University of South Carolina School of Medicine

**Tim Borden, Ph.D.**

*Doctorate in History from Indiana University, and is an inspector with the U.S. Bureau of Customs and Border Protection*  
Toledo, Ohio

**Brian Cobb, Ph.D.**

*Bioscience writer, researcher*  
Institute for Molecular and Human Genetics  
Georgetown University, Washington, D.C.

**Cecilia Colomé, Ph.D.**

*Astrophysicist, translator, and science writer*  
Austin, Texas

**Laurie Duncan, Ph.D.**

*Geologist, science writer, and researcher*  
Austin, Texas

**William J. Engle, P.E.**

*Writer on contemporary geophysics issues and the impacts of science and technology on history*  
Exxon-Mobil Oil Corporation (Rt.) New Orleans, Louisiana

**Antonio Farina, M.D., Ph.D.**

*Physician, researcher, and writer on medical science issues*  
Assistant Professor, University of Bologna, Italy

**Christopher T. Fisher, Ph.D.**

*Assistant Professor, Department of African American Studies and the Department of History*  
The College of New Jersey, Ewing, New Jersey

**Larry Gilman, Ph.D.**

*Electrical engineer and science writer*  
Sharon, Vermont

**William Haneberg, Ph.D.**

*Former research scientist and professor, now an independent consulting geologist and science writer*  
Portland, Oregon

**Brian D. Hoyle, Ph.D.**

*Science writer and Chief Microbiologist, Government of New Brunswick from 1993 to 1997*  
Nova Scotia, Canada

**Joseph Patterson Hyder**

*Writer on the historical impacts of science and technology*  
University of Tennessee College of Law, Knoxville, Tennessee

**Alexandr Ioffe, Ph.D.**

*Writer on the history of science and researcher with the Geological Institute of Russian Academy of Sciences in Moscow*  
Russian Academy of Sciences, Moscow

**Judson Knight**

*Science writer, researcher, and editor*  
Knight Agency Research Services, Atlanta, Georgia

**Michael Lambert, Ph.D.**

*Researcher at the Great Plains/Rocky Mountain Hazardous Substance Research Center and at the U.S. Naval Research Laboratory*  
Manhattan, Kansas

**Adrienne Wilmoth Lerner**

*Writer of various articles on the history of science, archaeology, and the evolution of security-related law*  
University of Tennessee College of Law, Knoxville, Tennessee

**Agnes Lichanska, Ph.D.**

*Science writer who has conducted research at the Department of Medical Genetics and Ophthalmology at Queen's University of Belfast (Northern Ireland)*

University of Queensland, Brisbane, Australia

**Eric v.d. Luft, Ph.D., M.L.S.**

*Writer on cultural, scientific, and intellectual history, and philosophy*

Curator of Historical Collections  
SUNY Upstate Medical University, Syracuse, New York

**Martin Manning**

*Served on the Economic Security Team, Office of International Information Programs, U.S. Department of State*

Bureau of Public Diplomacy  
U.S. Department of State, Washington, D.C.

**Kelli Miller**

*Served as news writer and producer for Inside Science TV News at the American Institute of Physics (AIP) and as executive producer of Discoveries & Breakthroughs Inside Science*

Atlanta, Georgia

**Caryn E. Neumann**

*Instructor and doctoral candidate in the Department of History at Ohio State University*

Columbus, Ohio

**Mike O'Neal, Ph.D.**

*Independent scholar and writer*

Moscow, Idaho

**Belinda M. Rowland, Ph.D.**

*Science and medical writer*

Voorheesville, New York

**Judyth Sassoon, Ph.D., ARCS**

*Science writer with research experience in NMR and X-ray crystallography techniques*

Department of Biology & Biochemistry  
University of Bath, United Kingdom

**Morgan Simpson**

*Aerospace Engineer*

National Aeronautical and Space Administration (NASA)

Kennedy Space Center, Cape Canaveral, Florida

**Constance K. Stein, Ph.D.**

*Writer on medical and bioscience issues related to modern genetics*

Director of Cytogenetics, Assistant Director of Molecular Diagnostics

SUNY Upstate Medical University, Syracuse, New York

**Tabitha Sparks, Ph.D.**

*Marion L. Brittain fellow, Georgia Institute of Technology and Fellow, Center for Humanistic Inquiry, Emory University*

Atlanta, Georgia

**David Tulloch**

*Science and technology writer*

Wellington, New Zealand

**Michael T. Van Dyke, Ph.D.**

*Served as visiting assistant professor, Department of American Thought & Language*

Michigan State University, East Lansing, Michigan

**Stephanie Watson**

*Science writer specializing in the social impacts of science and technology*

Smyrna, Georgia

**Simon Wendt, Ph.D.**

*Ph.D. candidate in Modern History and History instructor*

John F. Kennedy Institute for North American Studies, Free University of Berlin, Germany



# ||||| List of Entries |||||

## I A I

Abu Nidal Organization (ANO)  
Abu Sayyaf Group (ASG)  
Abwehr  
ADFGX Cipher  
Aflatoxin  
Africa, Modern U.S. Security Policy and Interventions  
Agent Orange  
Air and Water Purification, Security Issues  
Air Force Intelligence, United States  
Air Force Office of Special Investigations, United States  
Air Marshals, United States  
Air Plume and Chemical Analysis  
Aircraft Carrier  
Airline Security  
Al-Aqsa Martyrs Brigade  
Alex Boncayao Brigade (ABB)  
Al-Gama'a al-Islamiyya (Islamic Group, IG)  
Al-Ittihad al-Islami (AIAI)  
Al-Jama'a al-Islamiyyah al-Muqatilah bi-Libya  
Al-Jihad  
Allied Democratic Forces (ADF)  
Al-Qaeda (also known as Al-Qaida)  
Americas, Modern U.S. Security Policy and Interventions  
Ames (Aldrich H.) Espionage Case  
Anthrax  
Anthrax, Terrorist Use as a Biological Weapon  
Anthrax Vaccine  
Anthrax Weaponization  
Antiballistic Missile Treaty  
Antibiotics  
Anti-Imperialist Territorial Nuclei (NTA)  
APIS (Advance Passenger Information System)  
Archeology and Artifacts, Protection of during War  
Architecture and Structural Security  
Area 51 (Groom Lake, Nevada)  
Argentina, Intelligence and Security  
Argonne National Laboratory  
Armed Islamic Group (GIA)  
Arms Control, United States Bureau

Army for the Liberation of Rwanda (ALIR)  
Army Security Agency  
'Asbat al-Ansar  
Asilomar Conference  
Assassination  
Assassination Weapons, Mechanical  
Asymmetric Warfare  
ATF (United States Bureau of Alcohol, Tobacco, and Firearms)  
Atmospheric Release Advisory Capability (ARAC)  
Audio Amplifiers  
Aum Supreme Truth (Aum)  
Australia, Intelligence and Security  
Austria, Intelligence and Security  
Aviation Intelligence, History  
Aviation Security Screeners, United States

## I B I

B-2 Bomber  
B-52  
Bacterial Biology  
Ballistic Fingerprints  
Ballistic Missile Defense Organization, United States  
Ballistic Missiles  
Balloon Reconnaissance, History  
Basque Fatherland and Liberty (ETA)  
Bathymetric Maps  
Bay of Pigs  
Belgium, Intelligence and Security Agencies  
Belly Buster Hand Drill  
Berlin Airlift  
Berlin Tunnel  
Berlin Wall  
Biochemical Assassination Weapons  
Biocontainment Laboratories  
Biodetectors  
Bio-Engineered Tissue Constructs  
Bio-Flips  
Biological and Biomimetic Systems  
Biological and Toxin Weapons Convention  
Biological Input/Output Systems (BIOS)

- Biological Warfare  
 Biological Warfare, Advanced Diagnostics  
 Biological Weapons, Genetic Identification  
 Bio-Magnetics  
 Biomedical Technologies  
 Biometrics  
 Bio-Optic Synthetic Systems (BOSS)  
 Biosensor Technologies  
 BioShield Project  
 Bioterrorism  
 Bioterrorism, Protective Measures  
 Black Chamber  
 Black Ops  
 Black Tom Explosion  
 Bletchley Park  
 Bolivia, Intelligence and Security  
 Bomb Damage, Forensic Assessment  
 Bomb Detection Devices  
 Bombe  
 Bosnia and Herzegovina, Intelligence and Security  
 Botulinum Toxin  
 Brain-Machine Interfaces  
 Brain Wave Scanners  
 Brazil, Intelligence and Security  
 British Terrorism Act  
 Brookhaven National Laboratory  
 Bubonic Plague  
 Bugs (Microphones) and Bug Detectors  
 Bush Administration (1989–1993), United States  
     National Security Policy  
 Bush Administration (2001–), United States  
     National Security Policy
- C**
- Cambodian Freedom Fighters (CFF)  
 Cambridge University Spy Ring  
 Cameras  
 Cameras, Miniature  
 Canada, Counter-Terrorism Policy  
 Canada, Intelligence and Security  
 Canine Substance Detection  
 Carter Administration (1977–1981), United States  
     National Security Policy  
 CDC (United States Centers for Disease Control  
     and Prevention)  
 CERN  
 Chechen-Russian Conflict  
 Chemical and Biological Defense Information  
     Analysis Center (CBIAC)  
 Chemical and Biological Detection Technologies  
 Chemical Biological Incident Response Force,  
     United States  
 Chemical Safety and Hazard Investigation Board  
     (USCSB), United States  
 Chemical Safety: Emergency Responses  
 Chemical Warfare  
 Chemistry: Applications in Espionage, Intelligence,  
     and Security Issues  
 Chernobyl Nuclear Power Plant Accident, Detection  
     and Monitoring  
 Chile, Intelligence and Security  
 China, Intelligence and Security
- Chinese Espionage against the United States  
 Church Committee  
 CIA (United States Central Intelligence Agency)  
 CIA (CSI), Center for the Study of Intelligence  
 CIA Directorate of Science and Technology (DS&T)  
 CIA, Foreign Broadcast Information Service  
 CIA, Formation and History  
 CIA, Legal Restriction  
 Cipher Disk  
 Cipher Key  
 Cipher Machines  
 Cipher Pad  
 Civil Aviation Security, United States  
 Civil War, Espionage and Intelligence  
 Classified Information  
 Clinton Administration (1993–2001), United States  
     National Security Policy  
 Clipper Chip  
 Closed-Circuit Television (CCTV)  
 Coast Guard (USCG), United States  
 Coast Guard National Response Center  
 Code Name  
 Code Word  
 Codes and Ciphers  
 Codes, Fast and Scalable Scientific Computation  
 COINTELPRO  
 Cold War (1945–1950), The Start of the Atomic Age  
 Cold War (1950–1972)  
 Cold War (1972–1989): The Collapse of the Soviet  
     Union  
 Colombia, Intelligence and Security  
 Colossus I  
 COMINT (Communications Intelligence)  
 Commerce Department Intelligence and Security  
     Responsibilities, United States  
 Commission on Civil Rights, United States  
 Communicable Diseases, Isolation, and Quarantine  
 Communications System, United States National  
 Comprehensive Test Ban Treaty (CTBT)  
 Computer and Electronic Data Destruction  
 Computer Fraud and Abuse Act of 1986  
 Computer Hackers  
 Computer Hardware Security  
 Computer Keystroke Recorder  
 Computer Modeling  
 Computer Security Act (1987)  
 Computer Software Security  
 Computer Virus  
 Concealment Devices  
 Consumer Product Safety Commission (CPSC),  
     United States  
 Continuity Irish Republican Army (CIRA)  
 Continuity of Government, United States  
 Continuous Assisted Performance (CAP)  
 Coordinator for Counterterrorism, United States  
     Office  
 Copyright Security  
 Counterfeit Currency, Technology and the  
     Manufacture  
 Counter-Intelligence  
 Counter-Terrorism Rewards Program  
 Covert Operations  
 Crib  
 Crime Prevention, Intelligence Agencies

Critical Infrastructure  
 Critical Infrastructure Assurance Office (CIAO),  
 United States  
 Croatia, Intelligence and Security  
 Cruise Missile  
 Cryptology and Number Theory  
 Cryptology, History  
 Cryptonym  
 Cuba, Intelligence and Security  
 Cuban Missile Crisis  
 Customs Service, United States  
 Cyanide  
 Cyber Security  
 Cyber Security Warning Network  
 Czech Republic, Intelligence and Security

## I D I

D Notice  
 DARPA (Defense Advanced Research Projects  
 Agency)  
 Data Mining  
 DCI (Director of the Central Intelligence Agency)  
 DEA (Drug Enforcement Administration)  
 Dead Drop Spike  
 Dead-Letter Box  
 Decontamination Methods  
 Decryption  
 Defense Information Systems Agency, United  
 States  
 Defense Nuclear Facilities Safety Board, United  
 States  
 Defense Security Service, United States  
 Delta Force  
 Department of State Bureau of Intelligence and  
 Research, United States  
 Department of State, United States  
 DIA (Defense Intelligence Agency)  
 Dial Tone Decoder  
 Diplomatic Security (DS), United States Bureau  
 Dirty Tricks  
 Disinformation  
 DNA  
 DNA Fingerprinting  
 DNA Recognition Instruments  
 DNA Sequences, Unique  
 Document Destruction  
 Document Forgery  
 DOD (United States Department of Defense)  
 DOE (United States Department of Energy)  
 Domestic Emergency Support Team, United States  
 Domestic Intelligence  
 Domestic Preparedness Office (NDPO), United  
 States National  
 Doo Transmitter  
 Dosimetry  
 Double Agents  
 Drop  
 Drug Control Policy, United States Office of  
 National  
 Drug Intelligence Estimates  
 Dual Use Technology

## E E I

E-2C  
 Ebola Virus  
 E-Bomb  
 Echelon  
 Economic Espionage  
 Economic Intelligence  
 Egypt, Intelligence and Security  
 Eichmann, Adolf: Israeli Capture  
 Eisenhower Administration (1953–1961), United  
 States National Security Policy  
 El Salvador, Intelligence and Security  
 Electromagnetic Pulse  
 Electromagnetic Spectrum  
 Electromagnetic Weapons, Biochemical Effects  
 Electronic Communication Intercepts, Legal Issues  
 Electronic Countermeasures  
 Electronic Warfare  
 Electro-Optical Intelligence  
 Electrophoresis  
 EM Wave Scanners  
 Emergency Response Teams  
 Encryption of Data  
 Enduring Freedom, Operation  
 Energy Directed Weapons  
 Energy Regulatory Commission, United States  
 Federal  
 Energy Technologies  
 Engraving and Printing, United States Bureau  
 Engulf, Operation  
 Enigma  
 Entry-Exit Registration System, United States  
 National Security  
 Environmental Issues Impact on Security  
 Environmental Measurements Laboratory  
 EPA (Environmental Protection Agency)  
 Epidemiology  
 Espionage  
 Espionage Act of 1917  
 Espionage and Intelligence, Early Historical  
 Foundations  
 Estonia, Intelligence and Security  
 European Union  
 Executive Orders and Presidential Directives  
 Explosive Coal

## I F I

F-117A Stealth Fighter  
 FAA (United States Federal Aviation  
 Administration)  
 Facility Security  
 FBI (United States Federal Bureau of Investigation)  
 FCC (United States Federal Communications  
 Commission)  
 FDA (United States Food and Drug Administration)  
 Federal Protective Service, United States  
 Federal Reserve System, United States  
 FEMA (United States Federal Emergency  
 Management Agency)  
 FEST (United States Foreign Emergency Support  
 Team)

Fingerprint Analysis  
 Finland, Intelligence and Security  
 First of October Anti-fascist Resistance Group (GRAPO)  
 FISH (German *Geheimschreiber* Cipher Machine)  
 Fission  
 Flame Analysis  
 Flight Data Recorders  
 FM Transmitters  
 FOIA (Freedom of Information Act)  
 Food Supply, Counter-Terrorism  
 Ford Administration (1974–1977), United States National Security Policy  
 Foreign Assets Control (OFAC), United States Office  
 Foreign Intelligence Surveillance Act  
 Foreign Intelligence Surveillance Court of Review  
 Forensic Geology in Military or Intelligence Operations  
 Forensic Science  
 Forensic Voice and Tape Analysis  
 France, Counter-Terrorism Policy  
 France, Intelligence and Security  
 French Underground during World War II, Communication and Codes  
 Fusion

## | G |

G–2  
 GAO (General Accounting Office, United States)  
 Gas Chromatograph-Mass Spectrometer  
 General Services Administration, United States  
 Genetic Code  
 Genetic Information: Ethics, Privacy and Security Issues  
 Genetic Technology  
 Genomics  
 Geologic and Topographical Influences on Military and Intelligence Operations  
 Geospatial Imagery  
 Germany, Counter-Terrorism Policy  
 Germany, Intelligence and Security  
 Gestapo  
 GIS  
 Global Communications, United States Office  
*Glomar Explorer*  
 Government Ethics (USOGE), United States Office  
 GPS  
 Great Game  
 Greece, Intelligence and Security  
 GSM Encryption  
 Guatemala, Intelligence and Security  
 Guerilla Warfare

## | H |

HAMAS (Islamic Resistance Movement)  
 Hanssen (Robert) Espionage Case  
 Harakat ul-Jihad-I-Islami (HUJI) (Movement of Islamic Holy War)

Harakat ul-Jihad-I-Islami/Bangladesh (HUJI-B) (Movement of Islamic Holy War)  
 Harakat ul-Mujahidin (HUM) (Movement of Holy Warriors)  
 Hardening  
 Health and Human Services Department, United States  
 Heavy Water Technology  
 Hemorrhagic Fevers and Diseases  
 Hizballah (Party of God)  
 Homeland Security, United States Department of  
 HUMINT (Human Intelligence)  
 Hungary, Intelligence and Security  
 Hypersonic Aircraft

## | I |

IBIS (Interagency Border Inspection System)  
 IDENT (Automated Biometric Identification System)  
 Identity Theft  
 IFF (Identification Friend or Foe)  
 IMF (International Monetary Fund)  
 IMINT (Imagery Intelligence)  
 India, Intelligence and Security  
 Indonesia, Intelligence and Security  
 Infectious Disease, Threats to Security  
 Information Security  
 Information Security (OIS), United States Office of Information Warfare  
 Infrared Detection Devices  
 Infrastructure Protection Center (NIPC), United States National  
 INS (United States Immigration and Naturalization Service)  
 INSCOM (United States Army Intelligence and Security Command)  
 INSPASS (Immigration and Naturalization Service Passenger Accelerated Service System)  
 Inspector General (OIG), Office of the Intelligence  
 Intelligence Agent  
 Intelligence and Counterespionage Careers  
 Intelligence and Democracy: Issues and Conflicts  
 Intelligence and International Law  
 Intelligence and Law Enforcement Agencies  
 Intelligence & Research (INR), United States Bureau of  
 Intelligence Authorization Acts, United States Congress  
 Intelligence Community  
 Intelligence Literature  
 Intelligence Officer  
 Intelligence Policy and Review (OIPR), United States Office of  
 Intelligence Support, United States Office of Intelligence, United States Congressional Oversight of  
 Interagency Security Committee, United States  
 Internal Revenue Service, United States  
 International Atomic Energy Agency (IAEA)  
 International Narcotics and Law Enforcement Affairs (INL), United States Bureau of

Internet  
 Internet: Dynamic and Static Addresses  
 Internet Spam and Fraud  
 Internet Spider  
 Internet Surveillance  
 Internet Tracking and Tracing  
 INTERPOL (International Criminal Police Organization)  
 Interpol, United States National Central Bureau  
 Interrogation  
 Interrogation: Torture Techniques and Technologies  
 Iran-Contra Affair  
 Iran, Intelligence and Security  
 Iranian Hostage Crisis  
 Iranian Nuclear Programs  
 Iraq, Intelligence and Security Agencies in  
 Iraq War: Prelude to War (The International Debate Over the Use and Effectiveness of Weapons Inspections)  
 Iraq War (Immediate Aftermath)  
 Iraqi Freedom, Operation (2003 War Against Iraq)  
 Ireland, Intelligence and Security  
 Irish Republican Army (IRA)  
 Islamic Army of Aden (IAA)  
 Islamic Movement of Uzbekistan (IMU)  
 Isotopic Analysis  
 Israel, Counter-Terrorism Policy  
 Israel, Intelligence and Security  
 Italy, Intelligence and Security

## I J I

Jaish-e-Mohammed (JEM) (Army of Mohammed)  
 Japan, Intelligence and Security  
 Japanese Red Army (JRA)  
 JDAM (Joint Direct Attack Munition)  
 Jemaah Islamiya (JI)  
 Johnson Administration (1963–1969), United States National Security Policy  
 Joint Chiefs of Staff, United States  
 Jordan, Intelligence and Security  
 J-STARS  
 Justice Department, United States

## I K I

Kahane Chai (Kach)  
 Kennedy Administration (1961–1963), United States National Security Policy  
 Kenya, Bombing of United States Embassy  
 KGB (*Komitet Gosudarstvennoi Bezopasnosti*, USSR Committee of State Security)  
 Khobar Towers Bombing Incident  
 Knives  
 Korean War  
 Kosovo, NATO Intervention  
 Kumpulan Mujahidin Malaysia (KMM)  
 Kurdistan Workers' Party (PKK)  
 Kuwait Oil Fires, Persian Gulf War

## I L I

Language Training and Skills  
 Laser  
 Laser Listening Devices  
 Lashkar-e-Tayyiba (LT) (Army of the Righteous)  
 Law Enforcement, Responses to Terrorism  
 Law Enforcement Training Center (FLETC), United States Federal  
 Lawrence Berkeley National Laboratory (LBL)  
 Lawrence Livermore National Laboratory (LLNL)  
 League of Nations  
 Lebanon, Bombing of U.S. Embassy and Marine Barracks  
 Less-Lethal Weapons Technology  
 L-Gel Decontamination Reagent  
 Liberation Tigers of Tamil Eelam (LTTE)  
 Libraries and Information Science (NCLIS), United States National Commission on  
 Libya, Intelligence and Security  
 Libya, U.S. Attack (1986)  
 LIDAR (Light Detection and Ranging)  
 Lock-Picking  
 Locks and Keys  
 Looking Glass  
 Lord Haw-Haw  
 Lord's Resistance Army (LRA)  
 Los Alamos National Laboratory  
 Loyalist Volunteer Force (LVF)

## I M I

Mail Sanitization  
 Malicious Data  
 Manhattan Project  
 Mapping Technology  
 Marine Mammal Program  
 McCarthyism  
 Measurement and Signatures Intelligence (MASINT)  
 Metal Detectors  
 Meteorology and Weather Alteration  
 Mexico, Intelligence and Security  
 MI5 (British Security Service)  
 MI6 (British Secret Intelligence Service)  
 Microbiology: Applications to Espionage, Intelligence, and Security  
 Microchip  
 Microfilms  
 Microphones  
 Microscopes  
 Microwave Weaponry, High Power (HPM)  
 Middle East, Modern U.S. Security Policy and Interventions  
 Military Police, United States  
 MOAB (Massive Ordnance Air Burst Bomb)  
 Molecular Biology: Applications to Espionage, Intelligence, and Security  
 Moles  
 Monroe Doctrine  
 Morocco, Intelligence and Security  
 Mossad  
 Motion Sensors

Mount Weather  
 Movies, Espionage and Intelligence Portrayals  
 Mujahedin-e Khalq Organization (MEK or MKO)  
 Mustard Gas

## I N I

NAIS (National Automated Immigration Lookout System)  
 Nanotechnology  
 Napoleonic Wars, Espionage during  
 NASA (National Air and Space Administration)  
 National Archives and Records Administration (NARA), United States  
 National Command Authority  
 National Drug Threat Assessment  
 National Information Infrastructure Protection Act, United States  
 National Intelligence Estimate  
 National Interagency Civil-Military Institute (NICI), United States  
 National Liberation Army (ELN)—Colombia  
 National Military Joint Intelligence Center  
 National Preparedness Strategy, United States  
 National Response Team, United States  
 National Security Act (1947)  
 National Security Advisor, United States  
 National Security Strategy, United States  
 National Security Telecommunications Advisory Committee  
 National Telecommunications Information Administration, and Security for the Radio Frequency Spectrum, United States  
 NATO (North Atlantic Treaty Organization)  
 Natural Resources and National Security  
 Navy Criminal Investigative Service (NCIS)  
 NCIX (National Counterintelligence Executive), United States Office of the  
 NDIC (Department of Justice National Drug Intelligence Center)  
 Near Space Environment  
 Nerve Gas  
 Netherlands, Intelligence and Security  
 New People's Army (NPA)  
 New Zealand, Intelligence and Security  
 NFIB (United States National Foreign Intelligence Board)  
 NIC (National Intelligence Council)  
 Nicaragua, Intelligence and Security  
 Nigeria, Intelligence and Security  
 Night Vision Scopes  
 NIH (National Institutes of Health)  
 NIJ (National Institute of Justice)  
 NIMA (National Imagery and Mapping Agency)  
 NIMH (National Institute of Mental Health)  
 NIST (National Institute of Standards and Technology), United States  
 NIST Computer Security Division, United States  
 Nixon Administration (1969–1974), United States  
 National Security Policy  
 NMIC (National Maritime Intelligence Center)  
 NNSA (United States National Nuclear Security Administration)

NOAA (National Oceanic & Atmospheric Administration)  
 Noise Generators  
 Nongovernmental Global Intelligence and Security  
 Non-Proliferation and National Security, United States  
 NORAD  
 North Korea, Intelligence and Security  
 North Korean Nuclear Weapons Programs  
 Norway, Intelligence and Security  
 NRO (National Reconnaissance Office)  
 NSA (United States National Security Agency)  
 NSC (National Security Council)  
 NSC (National Security Council), History  
 NSF (National Science Foundation)  
 NTSB (National Transportation Safety Board)  
 Nuclear Detection Devices  
 Nuclear Emergency Support Team, United States  
 Nuclear Power Plants, Security  
 Nuclear Reactors  
 Nuclear Regulatory Commission (NRC), United States  
 Nuclear Spectroscopy  
 Nuclear Weapons  
 Nuclear Winter  
 Nucleic Acid Analyzer (HANAA)

## I O I

Oak Ridge National Laboratory (ORNL)  
 Official Secrets Act, United Kingdom  
 OPEC (Organization of Petroleum Exporting Countries)  
 Operation Liberty Shield  
 Operation Magic  
 Operation Mongoose  
 Operation Shamrock  
 Orange Volunteers (OV)  
 OSS (United States Office of Strategic Services)

## I P I

P-3 Orion Anti-Submarine Maritime Reconnaissance Aircraft  
 Pacific Northwest National Laboratory  
 Pakistan, Intelligence and Security  
 Palestine Islamic Jihad (PIJ)  
 Palestine Liberation Front (PLF)  
 Palestinian Authority, Intelligence and Security  
 PanAm 103, (Trial of Libyan Intelligence Agents)  
 Panama Canal  
 Parabolic Microphones  
 Pathogen Genomic Sequencing  
 Pathogen Transmission  
 Pathogens  
 Patriot Act Terrorist Exclusion List  
 Patriot Act, United States  
 Patriot Missile System  
 Pearl Harbor, Japanese Attack on  
 People Against Gangsterism and Drugs (PAGAD)  
 Persian Gulf War  
 Peru, Intelligence and Security

Petroleum Reserves, Determination  
 PFIAB (President's Foreign Intelligence Advisory Board)  
 Phoenix Program  
 Photo Alteration  
 Photographic Interpretation Center (NPIC), United States National  
 Photographic Resolution  
 Photography, High-Altitude  
 Playfair Cipher  
 Plum Island Animal Disease Center  
 Poland, Intelligence and Security  
 Politics: The Briefings of United States Presidential Candidates  
 Pollard Espionage Case  
 Polygraphs  
 Polymerase Chain Reaction (PCR)  
 Popular Front for the Liberation of Palestine (PFLP)  
 Popular Front for the Liberation of Palestine-General Command (PFLP-GC)  
 Port Security  
 PORTPASS (Port Passenger Accelerated Service System)  
 Portugal, Intelligence and Security  
 Postal Security  
 Postal Service (USPS), United States  
 Potassium Iodide  
 President of the United States (Executive Command and Control of Intelligence Agencies)  
 Pretty Good Privacy (PGP)  
 Privacy: Legal and Ethical Issues  
 Profiling  
 Propaganda, Uses and Psychology  
 Pseudoscience Intelligence Studies  
 Psychotropic Drugs  
 Public Health Service (PHS), United States  
*Pueblo* Incident  
 Purple Machine

## I Q I

Quantum Physics: Applications to Espionage, Intelligence, and Security Issues

## I R I

RADAR  
 RADAR, Synthetic Aperture  
 Radiation, Biological Damage  
 Radio Direction Finding Equipment  
 Radio Frequency (RF) Weapons  
 Radioactive Waste Storage  
 Radiological Emergency Response Plan, United States Federal  
 Reagan Administration (1981–1989), United States National Security Policy  
 Real IRA (RIRA)  
 Reconnaissance  
 Red Code  
 Red Hand Defenders (RHD)  
 Red Orchestra  
 Remote Sensing

Retina and Iris Scans  
 Revolutionary Armed Forces of Colombia (FARC)  
 Revolutionary Nuclei  
 Revolutionary Organization 17 November (17 November)  
 Revolutionary People's Liberation Party/Front (DHKP/C)  
 Revolutionary Proletarian Initiative Nuclei (NIPR)  
 Revolutionary United Front (RUF)  
 Revolutionary War, Espionage and Intelligence  
 RF Detection  
 Ricin  
 Robotic Vehicles  
 Romania, Intelligence and Security  
 Room 40  
 Rosenberg (Ethel and Julius) Espionage Case  
 Russia, Intelligence and Security  
 Russian Nuclear Materials, Security Issues

## I S I

Sabotage  
 Salafist Group for Call and Combat (GSPC)  
 Salmonella and Salmonella Food Poisoning  
 Sandia National Laboratories  
 Sarin Gas  
 Satellite Technology Exports to the People's Republic of China (PRC)  
 Satellites, Non-Governmental High Resolution  
 Satellites, Spy  
 Saudi Arabia, Intelligence and Security  
 Scanning Technologies  
 SEAL Teams  
 Secret Service, United States  
 Secret Writing  
 Security Clearance Investigations  
 Security, Infrastructure Protection, and Counterterrorism, United States National Coordinator  
 Security Policy Board, United States  
 Seismograph  
 Seismology for Monitoring Explosions  
 Senate Select Committee on Intelligence, United States  
 Sendero Luminoso (Shining Path, or SL)  
 SENTRI (Secure Electronic Network for Travelers' Rapid Inspection)  
 September 11 Terrorist Attacks on the United States  
 Sequencing  
 Serbia, Intelligence and Security  
 Sex-for-Secrets Scandal  
 Ships Designed for Intelligence Collection  
 "Shoe Bomber"  
 Shoe Transmitter  
 Short-Wave Transmitters  
 SIGINT (Signals Intelligence)  
 Silencers  
 Skunk Works  
 Slovakia, Intelligence and Security  
 Slovenia, Intelligence and Security  
 Smallpox  
 Smallpox Vaccine

SOE (Special Operations Executive)  
 Soldier and Biological Chemical Command  
 (SBCCOM), United States Army  
 Solid-Phase Microextraction Techniques  
 Soman  
 SONAR  
 SOSUS (Sound Surveillance System)  
 South Africa, Intelligence and Security  
 South Korea, Intelligence and Security  
 Soviet Union (USSR), Intelligence and Security  
 Space Shuttle  
 Spain, Intelligence and Security  
 Spanish-American War  
 Special Collection Service, United States  
 Special Counsel and Security Related  
 “Whistleblower” Protection Issues, United States  
 Office  
 Special Operations Command, United States  
 Special Relationship: Technology Sharing between  
 the Intelligence Agencies of the United States  
 and United Kingdom  
 Spectroscopy  
 Spores  
 SR-71 Blackbird  
 START I Treaty  
 START II  
 STASI  
 Stealth Technology  
 Steganography  
 Strategic Defense Initiative and National Missile  
 Defense  
 Strategic Petroleum Reserve, United States  
 Sudan, Intelligence and Security  
 Suez Canal  
 Supercomputers  
 Surgeon General and Nuclear, Biological, and  
 Chemical Defense, United States Office  
 Sweden, Intelligence and Security  
 Switzerland, Intelligence and Security  
 Syria, Intelligence and Security

## III

Tabun  
 Taiwan, Intelligence and Security  
 Taser  
 Technical Intelligence  
 Technology Transfer Center (NTTC), Emergency  
 Response Technology Program  
 Telemetry  
 Telephone Caller Identification (Caller ID)  
 Telephone Recording Laws  
 Telephone Recording System  
 Telephone Scrambler  
 Telephone Tap Detector  
 Terror Alert System, United States  
 Terrorism, Domestic (United States)  
 Terrorism, Intelligence Based Threat and Risk  
 Assessments  
 Terrorism, Philosophical and Ideological Origins  
 Terrorism Risk Insurance  
 Terrorist and Para-State Organizations  
 Terrorist Organization List, United States

Terrorist Organizations, Freezing of Assets  
 Terrorist Threat Integration Center  
 Thin Layer Chromatography  
 TIA (Terrorism Information Awareness)  
 Tissue-Based Biosensors  
 Tokyo Rose  
 Toxicology  
 Toxins  
 Tradecraft  
 Transportation Department, United States  
 Treasury Department, United States  
 Truman Administration (1945–1953), United States  
 National Security Policy  
 Truth Serum  
 Tularemia  
 Tunisian Combatant Group (TCG)  
 Tupac Amaru Revolutionary Movement (MRTA)  
 Turkey, Intelligence and Security  
 Turkish Hizballah  
 Typex

## II

U-2 Incident  
 U-2 Spy Plane  
 Ukraine, Intelligence and Security  
 Ulster Defense Association/Ulster Freedom Fighters  
 (UDA/UVF)  
 Ultra, Operation  
 Underground Facilities, Geologic and Structural  
 Considerations in the Construction  
 Undersea Espionage: Nuclear vs. Fast Attack Subs  
 Unexploded Ordnance and Mines  
 United Kingdom, Counter-Terrorism Policy  
 United Kingdom, Intelligence and Security  
 United Nations Security Council  
 United Self-Defense Forces/Group of Colombia  
 (*AUC Autodefensas Unidas de Colombia*)  
 United States, Counter-Terrorism Policy  
 United States, Intelligence and Security  
 United States Intelligence, History  
 Unmanned Aerial Vehicles (UAVs)  
 Uranium  
 Uranium Depletion Weapons  
 USAMRICD (United States Army Medical Research  
 Institute of Chemical Defense)  
 USAMRIID (United States Army Medical Research  
 Institute of Infectious Diseases)  
 USS *Cole*  
 USS *Liberty*  
 USSTRATCOM (United States Strategic Command)

## III

Vaccination  
 Vaccines  
 Variola Virus  
 Venezuela, Intelligence and Security  
 Venona  
 Vietnam War  
 Viral Biology



Viral Exposure Therapy, Antiviral Drug  
Development  
Voice Alteration, Electronic  
Voice of America (VOA), United States  
Vozrozhdeniye Island, Soviet and Russian  
Biochemical Facility  
Vulnerability Assessments  
VX Agent

## I W I

Walker Family Spy Ring  
War of 1812  
Water Supply: Counter-Terrorism  
Watergate  
Weapon-Grade Plutonium and Uranium, Tracking  
Weapons of Mass Destruction

Weapons of Mass Destruction, Detection  
Windtalkers  
World Health Organization (WHO)  
World Trade Center, 1993 Terrorist Attack  
World Trade Center, 2001 Terrorist Attack  
World War I  
World War I: Loss of the German Codebook  
World War II  
World War II: Allied Invasion of Sicily and “The  
Man Who Never Was”  
World War II, The Surrender of the Italian Army  
World War II, United States Breaking of Japanese  
Naval Codes

## I Z I

Zoonoses

*This page intentionally left blank*



## F-117A Stealth Fighter

Striking and unusual in appearance, the birdlike F-117A Nighthawk is the world's first aircraft designed to make full use of stealth technology. Conceived and designed in just 31 months at the Lockheed Advanced Development Projects "Skunk Works" in Burbank, California, the Nighthawk was built for the United States Air Force between 1982 and 1990. The single-seat, twin-engine F-117 was the only U.S. or coalition aircraft to strike targets in downtown Baghdad during the Persian Gulf War.

Both the air force and Lockheed are understandably reticent regarding the specific stealth technologies that make the Nighthawk virtually invisible to radar. However, it appears that the plane's distinctive shape serves to deflect radar waves, and that the materials used in building the craft absorb electromagnetic energy.

As befits an extraordinary aircraft, even the story of its birth is something of a saga: from the initial production decision in 1978 to the first test flight on June 18, 1981 was less than three years, lightning-quick for an undertaking of such magnitude. The speed of production has been credited not only to the engineers at the "Skunk Works," but also to the management team at the Aeronautical Systems Center at Wright-Patterson Air Force Base in Ohio.

The F-117A was not an aircraft the United States was inclined to share, even with allies, and therefore the only F-117A unit in the world is the 49th Fighter Wing (formerly the 4450th Tactical Group) at Holloman Air Force Base in New Mexico. Designed to deliver laser-guided weapons against critical targets, the F-117A has quadruple redundant fly-by-wire controls, and is equipped with a variety of sophisticated navigation and attack systems integrated into its digital avionics suite.

Capable of being refueled in the air, the F-117A flew 18.5 hours nonstop from Holloman to Kuwait during Operation Desert Storm in 1991, setting a record for single-seat

fighters. The aircraft was also deployed in Operation Allied Force in 1999, when it led the first North Atlantic Treaty Organization (NATO) strike against Yugoslavia on March 24. Additionally, the Nighthawk was selected to strike targets in downtown Baghdad in Operation Iraqi Freedom in 2003, not only because its invisibility to radar made it the safest craft to use, but also because its extraordinary accuracy made it capable of performing its job with minimal harm to innocent bystanders.

### ■ FURTHER READING:

#### BOOKS:

Aronstein, David C., and Albert C. Piccirillo. *Have Blue and the F-117A: Evolution of the "Stealth Fighter"*. Reston, VA: American Institute of Aeronautics and Astronautics, 1997.

Lake, Jon. *Jane's How to Fly and Fight in the F-117A Stealth Fighter*. London: HarperCollins Publishers, 1997.

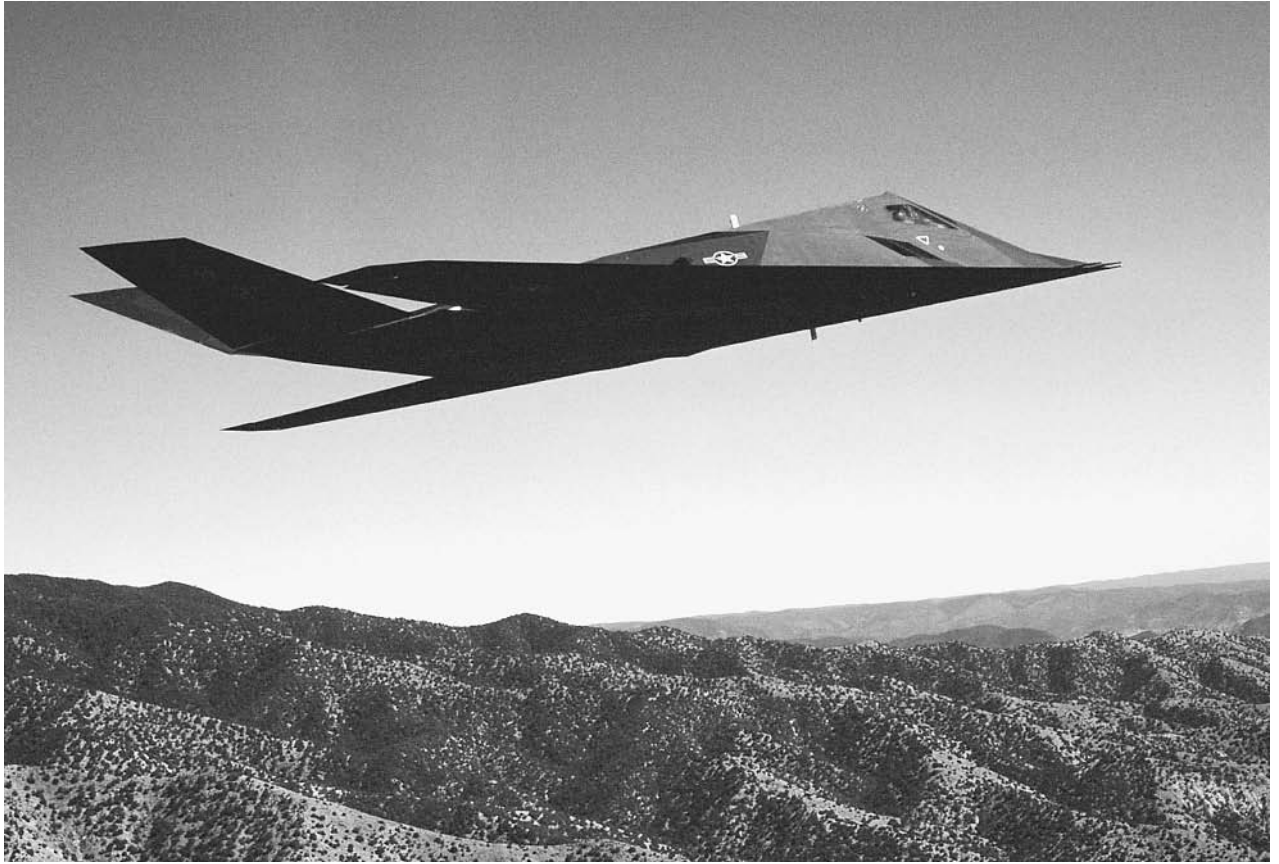
Macy, Robert, and Melinda Macy. *Destination Baghdad: The Story of the F-117A Stealth Fighter, the Plane Credited with Ripping out the Eyes and the Heart of the Iraqi War Machine, as Told by the Pilots who Flew the Most Dangerous Missions of Operation Desert Storm*. Las Vegas, NV: M&M Graphics, 1991.

#### ELECTRONIC:

F-117A Nighthawk. United States Air Force. <[http://www.af.mil/news/factsheets/F\\_117A\\_Nighthawk.html](http://www.af.mil/news/factsheets/F_117A_Nighthawk.html)> (March 8, 2003).

#### SEE ALSO

*Persian Gulf War*  
*Skunk Works*  
*Stealth Technology*



An F-117A Nighthawk Stealth fighter flies over the New Mexico desert during a training mission. AP/WIDE WORLD PHOTOS.

## FAA (United States Federal Aviation Administration)

■ STEPHANIE WATSON

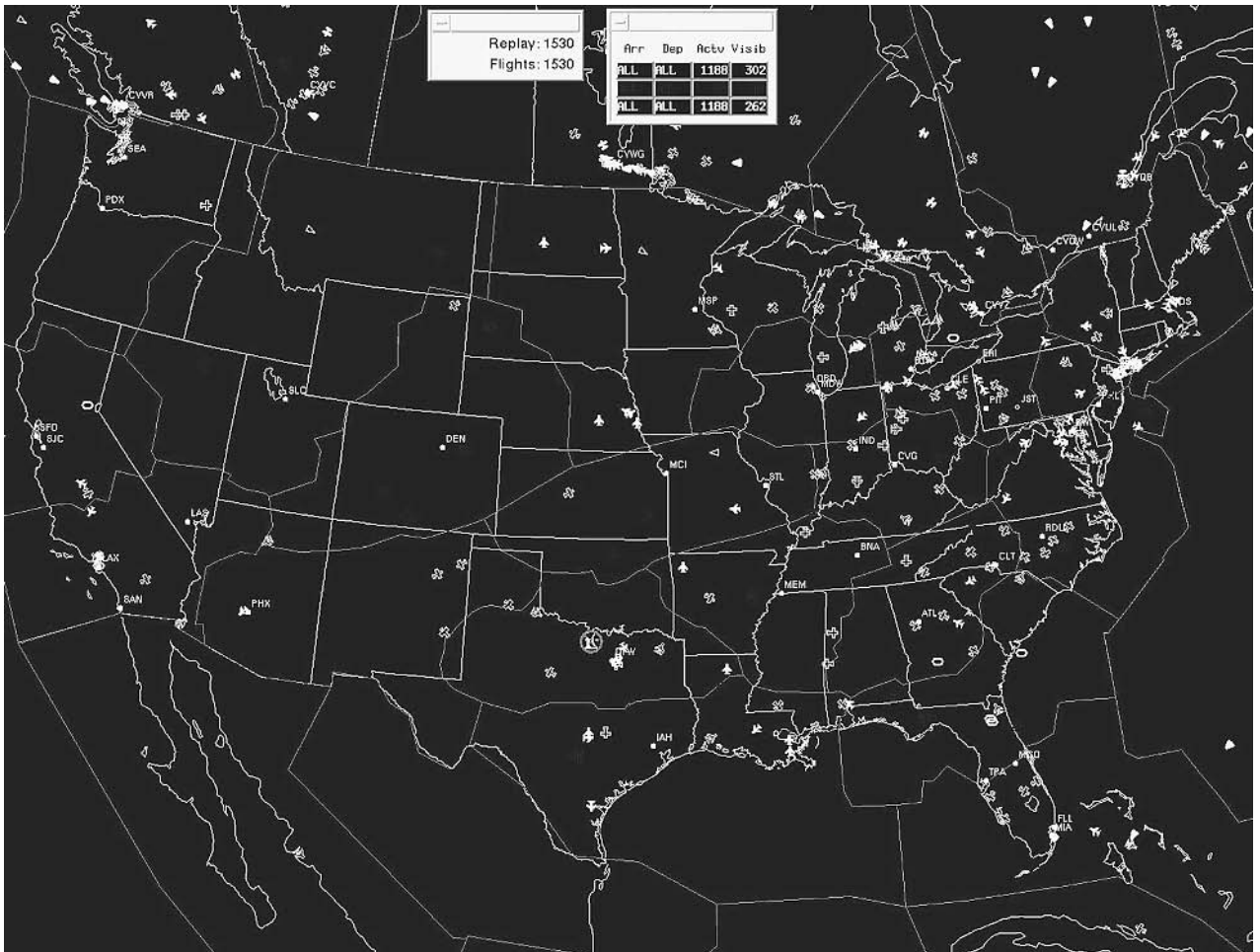
The Federal Aviation Administration (FAA) is the government agency charged with ensuring the safety of air travel in America, developing new aviation technologies, and overseeing air traffic control for both passenger and military aircraft.

**The FAA takes flight.** As air travel began to take off at the beginning of the 20th century, the government realized that a special agency was needed to regulate the fledgling airline industry. In 1926, Congress passed the Air Commerce Act, putting the U.S. Department of Commerce in charge of air travel and commerce. Under its wing emerged the earliest predecessor of the FAA, called the Aeronautics Branch. A former lawyer, William P. MacCracken, Jr., was chosen to head up the new agency. On April 6, 1927, MacCracken received the very first pilot's license. Three

months later, the agency issued the first aircraft mechanic's license.

In 1934, the Aeronautics Branch was renamed the Bureau of Air Commerce. Four years later, the oversight of civil aviation passed into the hands of an independent government agency, called the Civil Aeronautics Authority. President Franklin D. Roosevelt eventually split the authority into two agencies, the Civil Aeronautics Administration (CAA) and the Civil Aeronautics Board (CAB). The CAA issued pilot and aircraft certification, enforced safety regulations, and developed new air routes, while the CAB enacted safety rules, investigated crashes, and regulated the economic aspects of the airline industry.

America entered the jet age in the 1950s, with faster, more powerful airplanes that allowed the public to travel more easily and affordably. As more Americans took to the skies, the number of airplane crashes rose, and the government recognized the need for new aviation security measures. In 1958, Congress passed the Federal Aviation Act, creating the Federal Aviation Agency, which took over safety and air traffic control responsibilities from the CAA and CAB. When the organization became part of the new Department of Transportation in 1967, the word agency in the FAA's title was changed to administration.



Very light air traffic is shown at 11:30 a.m. on September 11, 2001, in this Federal Aviation Administration image. U.S. airspace was closed after hijacked airliners crashed into the World Trade Center towers and the Pentagon. AP/WIDE WORLD PHOTOS.

As the aviation industry and the world itself changed in the latter part of the 20th century, the role of the FAA evolved and expanded. A wave of hijackings in the 1960s gave a greater urgency to the need for more stringent passenger security standards. Concerns over the environment led to aircraft noise standards in 1968. Increasing air traffic led to the National Airspace System (NAS), a 1982 plan that modernized ground-to-air surveillance and communications systems.

Following the terrorist attacks on September 11, 2001, the FAA enacted tougher airport security measures, including background checks for all airport employees with access to secure areas, new rules prohibiting passengers from carrying on knives and other potential weapons, and more widespread use of explosive-detection machines for examining checked baggage. The agency also replaced privately owned airport security companies with federally employed screeners.

In April, 2003, the FAA announced that hardened cockpit doors had been retrofitted in over 10,000 foreign and domestic aircraft. The new doors are meant to deter

and stop small arms fire or forced entry, and can only be opened by the pilots from inside the cockpit.

**The FAA today.** The FAA is headquartered in Washington, D.C., with nine branches scattered across the country. Heading the agency is the administrator, who is assisted by a deputy administrator and six associate administrators. First and foremost, their job is to keep the skies over America safe. To that end, no aircraft can fly without first meeting the FAA's stringent safety standards, and no pilot can earn his or her wings without first receiving FAA certification. Mechanics, dispatchers, and flight instructors must be similarly certified. The agency also researches and develops new technologies to improve the quality of airplanes, navigation systems, and air traffic control communications systems and equipment. The FAA oversees a national network of some 450 airport towers, 21 air traffic control centers, and 61 flight service stations in the United States, and maintains close contact with international aviation agencies to ensure the safety of American passengers abroad.

## ■ FURTHER READING :

### BOOKS:

Preston, Edmund. *FAA Historical Chronology: Civil Aviation and the Federal Government, 1926–1996*. Washington: DOT/FAA, 1998.

Thompson, Scott A. *Flight Check! The Story of FAA Flight Inspection*. Washington: DOT/FAA, Office of Aviation System Standards, 1993.

### ELECTRONIC:

Federal Aviation Administration <<http://www1.faa.gov/>> (January, 20, 2003).

### SEE ALSO

*Air Marshals, United States*

*Airline Security*

*Aviation Security Screeners, United States*

*Civil Aviation Security, United States*

*September 11 Terrorist Attacks on the United States*

*Transportation Department, United States*

## Face Recognition Vendor Test (FRVT).

SEE *Biometrics*.

---

## Facility Security

---

Facility security is the protection, and the measures taken toward the protection, of a building or other physical location. Among the components of facility security are access control, or the protection against entry by unauthorized persons, fire detection and suppression, and emergency-response planning. Facility security planning involves both the use of personnel and technology, but though both are important, the quality, training, and trustworthiness of personnel is of greater significance ultimately than the sophistication of the equipment used to protect a facility.

**Personnel.** Facility security is the business both of government agencies and of private firms. The skills required for facility security work in the public and private sectors are essentially the same, and personnel with experience in one area are usually able to move easily into the other. Not all facility security personnel are the same: the more sensitive the area being guarded, and the more valuable or potentially dangerous its contents, the greater the skills required of the individuals who ensure its security.

One of the thorniest issues of personnel policy in facility security is pay, a factor that involves greater subtlety than initially meets the eye. Although there is not a direct correspondence or correlation between pay and honesty, in general, the higher the pay, the greater the amount of qualifications an employer can demand.

After the September 11, 2001, terrorist attacks, as the federal government began to reconsider the security screening process at airports, many observers questioned the reliability of security personnel.

**Qualifications.** An effective facility security officer must be of unquestionable honesty and trustworthiness, such that no amount of money or other inducements would be a temptation to betray an employer. The potential officer should expect to undergo background checks, which would typically be intensive on a level commensurate with the sensitivity of the job. These checks may include examination of the individual's financial and credit history; family and domestic history; arrest and police record, as well as other government records on the individual.

Whereas American citizens have a legal expectation of privacy, if not a constitutionally specified "right to privacy," such is not the case for an individual who offers his or her services to guard valuable or sensitive materials.

Beyond these considerations, a facility security officer should be resourceful, and capable of thinking in a non-linear fashion. He or she should be able to consider the possibility that a given action will have more than one possible result, and that a given event may have more than one possible cause. In testing the abilities of facility security personnel for highly sensitive roles, it is not enough that the officer be able to protect his or her facility from invasion: he or she should be capable of penetrating other facilities. Some private firms advertise the fact that their operatives have been able to penetrate supposedly secure buildings.

In a test of post-September 11 building security, government investigators were able to enter four federal buildings in Atlanta using false law enforcement identification equipment—a clear indication that those facilities were not properly protected by the personnel in place. As noted at the time in *Security Management*, the General Services Administration, which provided security for those federal buildings, was notorious for its low pay and minimal benefits, and this made it difficult to attract highly qualified personnel.

**Procedure and equipment.** Though the importance of personnel to facility security can hardly be overstated, people are not the only dimension. There are also procedure and equipment, though these can only be used to a degree of effectiveness commensurate with the capabilities of the security staff.

In the realm of procedure, there are necessary steps to be taken when securing areas containing valuable or potentially dangerous materials. It may be deemed wise, for instance, to keep sensitive areas and items as separated as possible, so as to maximize the amount of time and work necessary for an intruder to obtain the goods sought. On the other hand, a facility security plan may call for centralization of sensitive areas so as to maintain a closer watch on those areas.

Equipment may be necessary for access control, surveillance, detection, communication, and incident response. Access control can be as simple as a lock, or as high-tech as biometric scanning devices that read handprints or the iris of an individual's eye. Surveillance equipment usually involves cameras, and may be augmented by motion sensors, alarms, and other forms of equipment for detection.

Personnel must be equipped with devices for communicating with one another, and with a central monitoring station. In the event of a serious security breach or other incident, they should also be able to contact outside services. Communications equipment also aids in incident response, for which a facility security can also prepare with fire suppression items (handheld extinguishers and/or sprinklers installed on site), as well as first aid kits. Incident response, depending on the nature of the facility and the qualifications of the persons guarding it, may also require that personnel be equipped with weapons or defensive equipment such as tear gas.

## ■ FURTHER READING:

### BOOKS:

Kozlow, Christopher, and John P. Sullivan. *Jane's Facility Security Handbook*. Alexandria, VA: Jane's Information Group, 2000.

### PERIODICALS:

Gips, Michael A. "Options Reviewed for Federal Building Security." *Security Management* 46, no. 7 (July 2002): 14.

Thompson, Cheryl W. "Lawmaker Faults Nuclear Facility Security Policies." *Washington Post*. (March 25, 2002): A17.

Wolkowitz, Dave. "Facility Security—Playing It Safe." *Area Development Site and Facility Planning* 37, no. 9 (September 2002): 72.

### SEE ALSO

*Architecture and Structural Security*  
*Biological and Biomimetic Systems*  
*General Services Administration, United States Security Clearance Investigations*

## Fast Breeder Reactor.

SEE *Nuclear Reactors*.

# WARNING from the FBI

**The war against spies and saboteurs demands the aid of every American.**

**When you see evidence of sabotage, notify the Federal Bureau of Investigation at once.**

**When you suspect the presence of enemy agents, tell it to the FBI.**

**Beware of those who spread enemy propaganda! Don't repeat vicious rumors or vicious whispers.**

**Tell it to the FBI!**



*J. Edgar Hoover*  
J. Edgar Hoover, Director  
Federal Bureau of Investigation

The nearest Federal Bureau of Investigation office is listed on page one of your telephone directory.

An FBI poster signed by J. Edgar Hoover warns civilians against saboteurs and spies. ©CORBIS.

## FBI (United States Federal Bureau of Investigation)

■ ADRIENNE WILMOTH LERNER

The United States Federal Bureau of Investigation (FBI) is the nation's primary federal investigative service. The mission of the FBI is to uphold and enforce federal criminal laws, aid international, state, and local police and investigative services when appropriate, and to protect the United States against terrorism and threats to national interests.

The FBI employs nearly 30,000 men and women, including 12,000 special agents. The organization, headquartered in Washington, D.C., is field-oriented, maintaining a network of 56 domestic field offices, 45 foreign posts, and 400 satellite offices (resident agencies). The agency relies on both foreign and domestic intelligence information, to aid its anti-terror operations. As a law enforcement authority, the FBI only has jurisdiction in interstate, or federal, crimes.

## Origins and Formation of the FBI

In the nineteenth century, municipal and state governments shouldered the responsibility of law enforcement. State legislatures defined crimes, and criminals were prosecuted in local courts. The development of railroads and automobiles, coupled with advancements in communication technology, introduced a new type of crime that contemporary legal and law enforcement system was unequipped to handle. Criminals were able to evade the law by fleeing over state lines. To combat the growing trend of interstate crime, President Theodore Roosevelt proposed the creation of a federal investigative and law enforcement agency.

In 1908, Roosevelt and his attorney general, Charles Bonaparte, created a force of Special Agents within the Department of Justice. They sought the expertise of accountants, lawyers, Secret Service agents, and detectives to staff the ranks of the new investigative service. The new recruits reported for examination and training on July 26, 1908. This first corps of federal agents was the forerunner of the modern FBI.

When the federal bureau began operations, there were few federal crimes in the legal statutes. Federal agents investigated railroad scams, banking crimes, labor violations, and antitrust cases. The findings of their investigations, however, were usually disclosed to local or state law enforcement officials and courts for prosecution. In 1910, the federal government passed the Mann Act, expanding the jurisdiction of the investigation bureau by outlawing the transport of women over state lines for the purpose of prostitution. Granting federal agents the right to investigate, arrest, and prosecute persons in violation of the Mann Act solidified the interstate authority of federal investigative services.

The Special Agents force also aided border guards, investigating smuggling cases and immigration violations. At the outbreak of the Mexican revolution, bureau agents conducted limited espionage operations, gathering intelligence for the military and the government.

## World War I and the Interwar Years

When World War I erupted in Europe, the United States government, under President Woodrow Wilson, proclaimed American neutrality in the conflict. Despite the official declaration of neutrality, the United States increasingly aided Allied nations such as Britain and France with sales of weapons and supplies for the war effort. As a result, rival Germany sent saboteurs and spies into the United States to conduct espionage against United States military installations and ammunition factories. Several incidents, including an explosion near New York City, at Black Tom Pier, fanned public fear of German spies and saboteurs infiltrating the United States. Federal investigators were charged with investigating acts of terrorism and

sabotage, as well as ferreting out potential spies. For this job, Special Agents worked closely with military intelligence, gaining new law enforcement and espionage tradecraft skills.

With the entry of the United States into the European conflict, federal investigators gained jurisdiction over the enforcement of the Espionage, Sabotage, and Selective Service Acts. The bureau investigated alien enemies, and arrested men who dodged conscription.

After World War I ended in 1918, the force of Special Agents became the Bureau of Investigation. The agency gained considerable autonomy from Department of Justice oversight. During the 1920s, federal agents investigated several regional and national crime syndicates. Prohibition, the ban on sale and consumption of alcoholic beverages, prompted a rise in the illegal manufacture, trade, and sale of alcohol. Since the Department of the Treasury had jurisdiction over Prohibition violations, federal investigators worked closely with Treasury agents.

The interwar era was also marked by increased gangsterism. Gangsters posed a unique challenge to the Bureau of Investigation's narrow interstate jurisdiction. Many of the most notorious crime bosses were eventually arrested on charges of racketeering, tax evasion, or war profiteering. With no other means available, within their legal bounds, to bring down the resurgence of the often violent and well-armed Ku Klux Klan (KKK), the Bureau of Investigation targeted the leader of the Louisiana Klan for violations of the Mann Act.

The onset of the Great Depression helped escalate crime rates. The sour economy gave rise to increased labor violations, corruption, swindling, and murder. Two events, however, strengthened and expanded the Bureau of Investigation's jurisdiction. The kidnapping of the Lindbergh baby in 1932 prompted Congress to pass federal kidnapping statutes. Two years later, Congress passed legislation prohibiting the escape of criminals across state lines, providing for interstate extradition of criminals, and granting federal agents the right to investigate and arrest criminals who fled or operated across state lines. Further reforms of federal law enforcement services permitted agents to carry guns.

The structure of the agency changed dramatically in the 1920s and 1930s. J. Edgar Hoover assumed the directorship of the Bureau of Investigation. Hoover expanded the field office network from nine offices to over 30 offices within ten years. Agency personnel policy changed, requiring new agents to complete a rigorous, centralized training course. Promotions within the organization were secured through merit and consistency of service, not seniority. The agency still sought agent-recruits with training in accountancy and law, but expanded their search to include linguists, mathematicians, physicists, chemists, forensics specialists, and medical practitioners.

Technical advancements also changed agency operations. Basic forensic investigation began to be employed



in FBI crime scene investigations. The bureau established a fingerprint identification and index system in 1924. The national index assumed fingerprint records from state and local law enforcement agencies, as well as an older Department of Justice fingerprint registry dating back to 1905. The agency opened its first technical laboratory in 1932. The facility quickly expanded to cover a variety of forensic research, aiding investigators by comparing bullets, guns, tire tracks, watermarks, counterfeiting techniques, handwriting samples, and pathology reports.

## World War II and the Interwar Years

In 1935, the special task force of agents who formerly worked to combat Prohibition were separated from the agency, and the organization was renamed the Federal Bureau of Investigation (FBI). When war again broke out in Europe, FBI agents performed many of the same duties as they had during World War I. Before the United States entered the war in 1941, the FBI concentrated its efforts on locating, infiltrating, and dismantling political organizations sympathetic to German and Italian Fascism, and Soviet Communism, despite the latter nation's wartime alliance with Britain and France. President Franklin D. Roosevelt, and Secretary of State Cordell Hull, pushed for increased power for the FBI to investigate perceived subversives, even if these people were ordinary American citizens. A 1939 presidential directive, followed by the Smith Act of 1940, outlawed public advocacy of overthrowing the government.

When the United States entered the war after the bombing of Pearl Harbor, FBI agents aided national defense efforts by placing trained agents at key military and defense industry sites. Wartime agents received more intense training in counterintelligence measures, and the FBI established special counterintelligence units for covert operations at the government's discretion. FBI agents thwarted German and Japanese attempts at sabotaging national interests, including fuel reserves.

World War II also marked one of the darkest chapters of FBI operations. Despite opposition from FBI director Hoover, government officials declared all Japanese immigrants, and American citizens of Japanese descent, enemy aliens. The Japanese-American population on the West Coast was evicted from their homes and sent to internment camps for the duration of the war. Many lost homes and businesses that they were forced to leave behind. Since internment camps and enemy alien laws fell under federal jurisdiction, the FBI imposed curfews, administered deportations, and arrested those in violation of internment laws.

Conversely, FBI agents were the first federal authority since Reconstruction to enforce desegregation laws. Though segregation remained legal practice during the

1940s, the president appointed the Fair Employment Practices Commission (FEPC) to address concerns of African-American workers. FEPC possessed no enforcement authority, but FBI agents arrested several employers found in violation of the FEPC on the grounds of impeding the war effort.

## The FBI during the Cold War

**The early Cold War years.** When World War II ended in August 1945, increasingly hostile relations between the United States and the Soviet Union led to the Cold War, a diplomatic and military standoff that lasted over four decades. In the early Cold War years, the American government, and many members of the public, worried about the presence of Communist organizations and spies within the United States. The discovery of Soviet agents operating within government agencies, and the trial of individuals accused of stealing atomic secrets, and the test detonation of the first Soviet atomic bomb in 1949, fanned public anti-Communist hysteria. While the newly formed Central Intelligence Agency (CIA) worked to stop the expansion of the Soviet Union abroad, the FBI gained the post-war responsibility of defeating Communist organizations at home.

In the first fifteen years of the Cold War, the FBI investigations contributed to the McCarthy hearings, as well as high-profile spy cases like that of Julius and Ethel Rosenberg. The FBI gained the authority to conduct background checks on potential government employees, and investigate federal employees suspected of disloyal acts or espionage. The 1946 Atomic Energy Act gave the FBI jurisdiction over the secrecy and protection of atomic secrets. Legislation throughout the 1950s expanded the FBI's role to cover the security of atomic facilities, and defense industry sites.

In more routine law enforcement duties, the FBI continued to pursue interstate and federal criminals. In 1950, the agency published its first "Ten Most Wanted List."

**The early 1960s and the Civil Rights Movement.** Although the Cold War continued, the anti-Communist hysteria faded away in the late 1950s. FBI investigations of anti-government organizations and "subversive individuals" shifted with the political mood of the 1960s. The decade witnessed the assassination of President John F. Kennedy, the Vietnam War, and ushered in the Civil Rights Movement, both events signaled new duties and an expanded legal jurisdiction for the FBI.

When President Kennedy was assassinated in Dallas, Texas in 1963, the crime was legally a local homicide. No special legal provisions existed for the investigation of the assassination of a government official or the president. President Lyndon B. Johnson called in FBI agents to investigate the murder, setting the precedent for future legislation that designated assassination as a federal crime, and granted the agency jurisdiction in assassination cases.

The FBI was responsible for federal enforcement of the Civil Rights Act of 1964, and aiding desegregation efforts by investigating pro-segregation organizations and individuals. The FBI's charge to enforce civil rights legislation often put federal agents in conflict with local law enforcement officials, especially in the South and Midwest. Though the FBI routinely investigated violations of civil rights laws, they did not win the authority to prosecute violators through federal law until after 1966.

The FBI investigated, and helped prosecute criminals, in several high profile civil rights cases. Field agents in Louisiana and Mississippi investigated the murder of three voter registration workers in Philadelphia, Mississippi, before turning the case over to FBI headquarters in Washington, D.C. FBI agents conducted crime scene, forensics, and extended investigations of the assassinations of civil rights leaders Martin Luther King, Jr., and Medger Evers. They eventually arrested, aided the prosecution of, and gained convictions for the assassins, although Byron De La Beckwith, who shot Medger Evers, was not found guilty until 1994.

**The Vietnam and Watergate era.** The United States, in an attempt to stem Soviet influence in Asia, entered the Vietnam War. The war was controversial, with many young people opposing U.S. military intervention in the conflict. The re-institution of the draft further angered anti-war sympathizers. Government officials grew increasingly suspicious of anti-war organizations and the large demonstrations they organized. Though the vast majority of anti-war demonstrators and organizations advocated peaceful protest and civil disobedience, a few militant and extremist groups resorted to acts of violence and sabotage. The actions of these groups prompted the FBI to conduct widespread surveillance of the anti-war movement. Utilizing counterintelligence techniques, the FBI used a myriad of intrusive surveillance, known as "Cointelpro," methods to thwart terrorist action by radicals. However, some criticized the organization of conducting domestic espionage, especially on the peaceful majority of anti-war supporters. Hoover, still director of the FBI, responded by promoting passage of the Omnibus Crime Control Act, which limited the use of wiretaps, listening devices, clandestine photographs, and other surveillance methods. The act defined new operational procedures for FBI agents, and was the first legal compromise between intelligence and privacy interests.

In 1972, public attention shifted from the Vietnam conflict, to the actions of the Nixon administration. On June 17, 1972, five men were arrested while breaking into the Watergate apartment complex that housed the headquarters for the Democratic Party. Subsequent investigations by a special team of federal agents connected the men, most whom were former CIA and FBI agents, to the Office of the President. Despite the implication of a few FBI agents in the extensive cover-up operation that followed the break-in, FBI investigators cooperated with a specially appointed Senate investigatory committee, surrendering

all information pertaining to Watergate. The ensuing scandal, known as Watergate, not only forced the resignation of Nixon and most of his administration, but also damaged public faith in the government and its intelligence and security agencies.

**The end of the Cold War.** A period of Cold War détente in the 1980s allowed the FBI to concentrate on agency reforms and expansion of its domestic intelligence capabilities. In 1982, following a outburst of international terrorism, the director of the FBI, William Webster, made counterintelligence and anti-terrorism operations an agency priority. He established the National Center for the Analysis of Violent Crime, a facility that would conduct sophisticated forensic analysis on crimes. The renewed agency attention to counterintelligence discovered over 30 cases of espionage against the United States government in 1985.

Combating the rise of white-collar financial crimes and the drug trade were other priorities of the FBI during the 1980s. FBI investigations implicated high-ranking government officials in financial fraud and abuse of power scandals, including members of the Congress (ABSCAM), defense industry (ILL WIND), and judiciary (GREYLORD). Federal agents also investigated fraud cases during the savings and loan crisis.

## The Rise of Terrorism and the FBI Today

In 1991, the Soviet Union collapsed. Its formal dissolution on December 25, 1991, marked the end of the Cold War. In the decade that followed, the international political map drastically altered, changing the global balance of power and permitting the rise of new threats to United States national security. In response to the changing international environment, the FBI shifted the priority of its operations. Several key events, including the 1993 bombing of the World Trade Center by Islamist, foreign terrorists, and the 1995 bombing of a federal building in Oklahoma City by a domestic terrorist, prompted the FBI to restructure its counterintelligence and counter-terrorism operations.

To aid its current operations, the FBI embraced the use of several new technologies in its operations. The advent of personal computers and the Internet aided research and processing of investigation information. Searchable databases store information on suspects, crime statistics, fingerprints, and DNA samples. However, their use also created security risks that necessitated the creation of specialized information systems protection task forces. The agency created Computer Analysis and Response Teams (CART) to aid field investigators with the recovery of data from damaged or sabotaged electronic sources. In 1998, the establishment of the National Infrastructure Protection Center (NIPC) permitted the FBI to monitor the dissemination of computer viruses and worms.

Forensic use of DNA radically altered both the legal process and forensic research of FBI investigations. DNA analysis allows specialists to positively identify victims and perpetrators of crimes by comparing particular patterns in individual DNA. FBI forensic specialists created a national DNA databank in 1998 to aid ongoing investigations.

After the September 11, 2001, terrorist attacks on the United States, and subsequent anthrax attacks on national post offices and media outlets, the FBI expanded its counterintelligence and counter-terrorism operations to include anti-bioterror task forces. The FBI, working in conjunction for the Centers for Disease Control (CDC), employs agents to aid in the investigation and identification of bioterror agents, and law enforcement in the event of a bioterror attack. FBI analysis and research divisions have compiled massive databases on known biological agents, stockpiles of weapons, and terrorist groups who may possess biological weapons. FBI analysts develop profiles of terrorist groups to better understand their mindsets and possible future actions.

The FBI's focus on the prevention of terrorism failed to thwart the September 11, 2001, terrorist attacks on the World Trade Center and the Pentagon. However, FBI investigations successfully found and prosecuted the perpetrators of the Oklahoma City bombing and the 1993 attack on the World Trade Center. In its ongoing investigation of the events of September 11, FBI agents have found and arrested several persons suspected of having connections to the al-Qaeda terrorist network and the recent terrorist attacks. The FBI is also designated as the primary agency of enforcement for the Patriot Act.

Although no major FBI operations were assumed into the Department of Homeland Security (DHS), the establishment of pending DHS committees to govern intelligence agency cooperation and information sharing will alter the manner in which the FBI relays information to the President and other government officials. Proponents of the DHS hope the agency will streamline communication among intelligence and security agencies. Critics of proposed DHS intelligence reforms charge that agencies, such as the FBI, will lose investigative and operational autonomy. Despite the changing future of the structure of the United States intelligence community, the FBI will undoubtedly play a central role.

#### ■ FURTHER READING:

##### BOOKS:

Kessler, Ronald. *The Bureau: The Secret History of the FBI*. New York: St. Martin's Press, 2002.

##### ELECTRONIC:

United States Federal Bureau of Investigation. <<http://www.fbi.gov>> (May 2003).

##### SEE ALSO

*Anthrax, Terrorist Use as a Biological Weapon*

*Black Tom Explosion*  
*CIA (CSI), Center for the Study of Intelligence*  
*COINTELPRO*  
*Cold War (1945–1950), The Start of the Atomic Age*  
*Cold War (1950–1972)*  
*Cold War (1972–1989): The Collapse of the Soviet Union*  
*Commission on Civil Rights, United States*  
*Counter-Intelligence*  
*Counter-terrorism Policy, United States*  
*Infrastructure Protection Center (NIPC), United States*  
*National*  
*Justice Department, United States*  
*McCarthyism*  
*Pearl Harbor, Japanese Attack on*  
*Privacy: Legal and Ethical Issues*  
*September 11 Terrorist Attacks on the United States*

## FCC (United States Federal Communications Commission)

■ STEPHANIE WATSON

The Federal Communications Commission (FCC), an independent government agency, oversees the media and communications industries in the United States. Included under the FCC's jurisdiction are radio, television, cable, telephone, satellite, and wireless (cellular phones and pagers) providers. As part of their regulatory responsibilities, FCC commissioners review and grant broadcasting licenses, approve corporate mergers and acquisitions, and protect consumers by responding to complaints and investigating claims of unfair rates and fraudulent business practices.

In the wake of the September 11, 2001 terrorist attacks, the FCC tightened its focus on security, and began looking at new ways to protect the nation's communications infrastructure. In March of the following year, it announced the creation of a new Media Security and Reliability Council. The federal advisory committee, comprised of media company executives, public service representatives, trade association members, and manufacturers, meets regularly to evaluate the security of national communications networks, and to strategize measures to protect against future attacks.

The FCC is governed by five commissioners, who are appointed by the president with the Senate's approval. Rules governing the FCC stipulate that no more than three commissioners can be from the same political party. Each commissioner serves for a five-year period. The agency is funded by and reports to the United States Congress. The FCC chairman directs the organization's activities and is responsible for hiring its bureau chiefs and department heads.

The FCC is divided into six bureaus, each of which has been designated to provide a specific function. The Media

Bureau regulates and licenses broadcast television and radio stations, cable and satellite providers; the Wireless Telecommunications Bureau oversees cellular phones, pagers, and two-way radios; the Consumer and Governmental Affairs Bureau educates the public and coordinates with other government agencies to protect consumer interests; the Enforcement Bureau carries out the rules set forth under the Communications Act; the International Bureau directs communications activities outside the United States; and the Wireline Competition Bureau regulates telephone companies that provide interstate and intrastate wire-based service. Ten staff offices have been set up to support these bureaus.

**The birth of the FCC.** The FCC was set up under the 1934 Communications Act to regulate radio and telephone communications. It combined functions originally designated to the Federal Radio Commission, Interstate Commerce Commission, and Postmaster General. As the television, cable and wireless industries emerged in subsequent years, the FCC's reach was extended and its responsibilities increased. New regulations were enacted to govern each new industry, for example the Communications Satellite Act of 1962 and the Cable Act of 1992.

Each industry under the FCC's jurisdiction was originally designated a separate entity, and prohibited by the government from crossing over into each other's territory. That is, until Congress signed the landmark 1996 Telecommunications Act. The act relaxed the rules governing corporate ownership within the telephone, television, and computer industries; allowing, for example, local phone companies to offer long-distance service and cable companies to offer Internet access. The move allowed greater competition among companies, and more choice and protection against monopolistic pricing practices for consumers. It also set the stage for a host of media mergers and acquisitions, most notably: America Online/Time Warner/Turner Broadcasting system, and ABC/Walt Disney Co., and MCI/Worldcom.

Over the years, the FCC has directed a number of important initiatives. In the early 1960s, when then-chairman Newton Minnow called television "a vast wasteland," television stations were spurred to raise programming standards. In 1990, the Children's Television Act limited advertising in programs geared to children and made children's programming a stipulation for license renewal. The FCC has also had to deal with First Amendment issues, for example obscenity cases relating to the music industry and radio broadcasts by so-called "shock jocks."

#### ■ FURTHER READING:

##### BOOKS:

Fleissner, Jennifer *The Federal Communications Commission*. New York: Chelsea House Publishers, 1992.

Hilliard, Robert L. *The Federal Communications Commission: A Primer*. Boston: Focal Press 1991.

Paglin, Max D., ed. *A Legislative History of the Communications Act of 1934*. New York: Oxford University Press, 1990.

##### PERIODICALS:

Hickey, Neil. "So Big: The Telecommunications Act at Year One." *Columbia Journalism Review* Jan/Feb. 1997: 23–28.

##### ELECTRONIC:

The Federal Communications Commission <<http://www.fcc.gov/>> (January 30, 2003).

##### SEE ALSO

*Communications System, United States National Electronic Communication Intercepts, Legal Issues National Telecommunications Information Administration, and Security for the Radio Frequency Spectrum, United States Telephone Recording Laws*

## FDA (United States Food and Drug Administration)

The Food and Drug Administration (FDA), a Department of Health and Human Services agency, regulates the development, sale, and distribution of food products, prescription and over-the-counter drugs, cosmetics, and medical equipment. The FDA's reach is so extensive that one-fifth of all consumer dollars spent in the U.S. purchase a product regulated by the FDA. The goal of the FDA is to protect consumers by ensuring the safety of food and drug products sold in the U.S.

The FDA traces its history to 1862, when President Abraham Lincoln created a chemistry division under the Department of Agriculture. Congress created the modern FDA in 1906 with the passage of the Food and Drugs Act. The 1906 law gave limited power to the FDA to monitor the safety of food and drug products. In 1938, Congress expanded the power of the FDA by passing the Food, Drug, and Cosmetic Act. This act granted the FDA the power to test drugs and determine their safety and efficacy before allowing companies to sell the new drugs. The act also granted the FDA authority to regulate cosmetics.

While the FDA's primary task is to ensure food and drug safety, in recent years the agency has taken on an increased role in the fight against bioterrorism. The FDA is leading efforts to develop and produce vaccines and treatments plans to prevent or stop the spread of a bioterror attack. In this quest, the FDA must quickly test vaccines, so private companies can produce and stockpile vaccines.

The variety of possible pathogens (disease-causing microorganisms) that might be used in bioterrorism has tested the limits of the FDA. The administration must simultaneously assess the effectiveness of vaccines and treatments for anthrax, smallpox, botulism, plague, hemorrhagic fevers, and other potential bioweapons. Additionally, the FDA, in conjunction with the Centers for Disease Control, must take into account that terrorists might genetically alter existing pathogens to reduce the efficacy of current vaccines and treatments. The FDA plans to thwart potential terrorist attacks by expediting its approval process for new vaccines and drugs that could reduce the severity of a bioterror attack.

#### ■ FURTHER READING :

##### ELECTRONIC:

Department of Health and Human Services. "United States Food and Drug Administration." <<http://www.fda.gov>> (May 2003).

##### SEE ALSO

*Bioterrorism, Protective Measures*  
*Food Supply, Counter-Terrorism*  
*Salmonella and Salmonella Food Poisoning*  
*Vaccination*

---

## Federal Protective Service, United States

---

#### ■ CARYN E. NEUMANN

The United States Federal Protective Service (FPS) is the security arm of the General Services Administration (GSA) and it is responsible for the protection of most of the civilian workspace owned or leased by the federal government, as well as the safety of the workers and visitors who use these sites. Headquartered in Washington, D.C. since its 1949 founding, FPS guards more than 8000 sites and one million federal workers and visitors on a daily basis. It promotes safety by employing law enforcement, physical security, and investigative personnel as well as contract guards, electronic surveillance, entry control devices, and a crime prevention awareness campaign. The agency serves as a centralized communication provider by networking with federal, state, and local law enforcement agencies.

The mission of FPS is to permit the conduct of government business by ensuring a safe environment that is open and inviting in a professional and cost effective

manner. The agency traces its origins to the Federal Property and Administrative Services Act of 1949, which consolidated real property functions within the newly created GSA and brought the U.S. Special Police under the protection division of the GSA's Public Building Service. In 1971, GSA established the Federal Protective Force, which later became FPS, in response to the growing number of demonstrations occurring at federal facilities. FPS covers buildings housing most federal agencies, committees, and commissions; U.S. District and Appellate Courts; and U.S. senators and congressional representatives. It bears responsibility for the protection of U.S. Border Patrol Stations, including the San Ysidro Border Station, which separates Tijuana, Mexico from San Diego, California and is considered to be the busiest land port in the world.

Over the years, FPS has shifted its emphasis from the fixed guardpost concept of security to a mobile police force that promotes physical security and crime prevention. The agency has recently adopted community policing, which means that it has moved its officers out of vehicles to allow them to spend more time in and around the buildings leased and operated by GSA. FPS coordinates regional activities with control centers in New York, Boston, Philadelphia, Atlanta, Denver, Chicago, San Francisco, Seattle, Fort Worth, Kansas City, and Washington, D.C. as well as branches in the Far East and Caribbean. It has additional offices in all fifty states plus Puerto Rico and the Virgin Islands.

To meet its responsibilities, FPS performs both security and law enforcement functions with uniformed and plainclothes personnel and regularly coordinates its activities with the Federal Emergency Management Agency (FEMA). Security, increasingly performed by contract guards as well as physical security specialists, includes such activities as the placement of security equipment and technology. FPS security personnel participate in the modification and repair of existing buildings as well as the construction of new ones to ensure that these sites have specially tailored security measures, equipment, and technology in place. FPS also routinely conducts building assessments of all GSA-controlled facilities to identify security weaknesses. Law enforcement security officers (LESOs), who hold the core FPS position, conduct preliminary investigations of accidents, incidents, and criminal complaints occurring on GSA-controlled property. LESOs do not investigate criminal offenses involving GSA employees but they are responsible for gathering protective intelligence information pertaining to demonstrations, bomb threats, and other criminal activities. FPS law enforcement personnel carry guns and are trained at the Federal Law Enforcement Training Center in Glynco, Georgia.

Until the 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City, FPS had suffered from repeated budgetary and personnel cuts that compromised its ability to guarantee the safety of federal workers and visitors. After the attack, the GSA bolstered all of its

security systems including FPS. As long as fear of terrorism remains strong, FPS will likely play a significant role in homeland security.

## ■ FURTHER READING:

### BOOKS:

United States Congress. Committee on Environment and Public Works. Subcommittee on Transportation and Infrastructure. *Federal Protective Service Reform Act of 2000: Hearing Before the Subcommittee on Transportation and Infrastructure on the Committee on Environment and Public Works, U.S. Senate, 106 Congress, second session, September 28, 2000 on H.R. 809, a Bill to Amend the Act of June 1, 1948 to Provide for the Reform of the Federal Protective Service*. Washington, D.C.: Government Printing Office, 2000.

United States General Services Administration. Office of Federal Protective Service. *Careers in Security and Law Enforcement*. Washington, D.C.: Government Printing Office, 2002.

———. Public Buildings Service. Law Enforcement Division. *The Federal Protective Service*. Washington, D.C.: Government Printing Office, 1998.

### SEE ALSO

*FEMA (United States Federal Emergency Management Agency) General Services Administration, United States Intelligence and Counter-Espionage Careers*

## Federal Reserve System, United States

### ■ JUDSON KNIGHT

Created by the passage of the Federal Reserve Act in 1913, the Federal Reserve System serves as the central bank of the United States. Commonly known as the Fed, it conducts monetary policy for the nation by exerting direct influence on the money supply, interest rates, and the purchase of government securities. It is the means by which federally issued currency and coinage reaches financial institutions, which receive these through the 12 Federal Reserve district banks located in various major cities throughout the United States. The Fed also sets the interest rate at which it loans money to member financial institutions, thus establishing a baseline for the rates of interest at which money is borrowed and lent throughout the United States.

### Conducting Monetary Policy

The initial mandate granted to the Federal Reserve System by Congress was to provide and ensure stability,

safety, and flexibility in the national monetary and financial system. Since 1913, the responsibilities and powers accorded to the Fed have grown considerably.

Today the Federal Reserve shapes, directs, and conducts U.S. monetary policy. Its overall concern is the well being of the national economy, which it seeks to achieve through a number of measurable goals, including price stability and full employment. These goals it achieves, in turn, through three principal means at its disposal: the control of the money supply by the issuance of currency to member financial institutions, the setting of interest rates at which it loans funds to those institutions, and the open market purchase of government securities.

**Controlling the money supply.** Under the Legal Tender Act of 1862, the United States began issuing currency notes, known as U.S. notes, through the Treasury Department, and continued to do so until January 21, 1971. At the time it passed the act, Congress set a limit of \$300 million on the value of U.S. notes that could be in circulation at any one time. Significant by the standards of the Civil War era, this sum represents a tiny portion of the funds in circulation today, which are known as Federal Reserve notes.

Whereas U.S. notes represented obligations of the federal government alone, Federal Reserve notes, authorized under the 1913 act that created the Fed itself, represent an obligation both of the federal government and the Federal Reserve system. The original Legal Tender Act was accordingly amended to include Federal Reserve notes as legal tender, meaning that they legally satisfy debts equal to the face value of the note tendered.

It is technically illegal to refuse legal tender (which today is synonymous with Federal Reserve notes) for services already rendered, though it is not illegal to refuse it for services not yet rendered. Therefore, a business that accepts only checks or credit must post a notice indicating this, so that the customer is aware of the fact prior to tendering payment.

**Setting interest rates.** In addition to controlling the money supply through the issuance of legal tender, the Federal Reserve directly affects monetary policy by a second and perhaps even more significant means: the setting of interest rates. This is accomplished by determining the discount rate, or the rate it charges member institutions for loans. These institutions, in turn, charge other depository institutions a certain rate for overnight loans of funds that are immediately available at the Federal Reserve Bank. The rate at which Fed member banks charge money to depository institutions, known as the federal funds rate, will always be slightly higher than the discount rate, but varies from institution to institution, and from day to day.

In order to turn a profit, banks that borrow money at the federal funds rate, in turn, charge borrowers—both



Guided by tradition, Federal Reserve Chairman Alan Greenspan assembles members of the Federal Open Market Committee around this 27-foot mahogany table eight times a year to set interest rates. AP/WIDE WORLD PHOTOS.

businesses and individuals—slightly higher rates. By this chain of relationships, the Fed exerts an all but direct influence on consumer credit costs ranging from the annual percentage rate on a credit card to the rate charged on a 30-year housing loan.

**Open market operations.** In addition to setting interest rates and controlling the money supply, the Fed conducts monetary policy through a third instrument, open market operations, or the buying and selling on the open market of securities issued by the U.S. Treasury and federal agencies. These securities include bonds of various types, as well as other government certificates. In each case, the value of the bond or certificate ultimately rests in the fiscal strength of the federal government.

Historically, the Federal Reserve has tied its objectives for open market operations either to a certain quantity of reserves, or a certain price. Prior to the administration of Federal Reserve Chairman Alan Greenspan, who was appointed by President Ronald Reagan in 1987, the Fed tended to focus on seeking a desired quantity of securities as reserves. Since that time, however, the Fed has sought to attain desirable levels in the price of securities, which are the federal funds rate. From 1995, it began

announcing target levels for the federal funds rate, which rose in the healthy economic climate of 1999 and 2000, but fell in the recessionary economies of 2001 and 2002.

## Maintaining Financial Stability

The open market operations of the Federal Reserve System are a clear means by which the Fed helps to maintain both financial and ultimately, political stability in the nation. Although it continually pursues its objective of ensuring stability through the three significant means at its disposal, the actions of the Federal Reserve become particularly evident during periods of financial upheaval.

The stock market crash of October, 1987, the Asian financial crisis and its aftermath in late 1998, and the terrorist attacks of September, 2001 each presented an occasion in which the U.S. financial system faced challenges, and when consumer faith in the national economy wavered. In each such situation, as well as in less significant crises, the Federal Reserve has gone into action, ensuring monetary liquidity through large balances of available cash; keeping interest rates manageable by extending discount loans to depository institutions; and setting the example of faith in U.S. institutions by purchasing government securities on the open market.

Even in times when the affairs of the nation are running more smoothly, the Fed continues to influence monetary policy. Americans are less likely to take note of the Federal Reserve in those situations, yet it is the Fed itself that deserves much of the credit for the stability in such times. The most visible means by which the Fed affects the economy is through the discount rate, which serves, in effect, like a gas pedal for economic growth. When rates are low, economic activity increases, and the economy grows. If the economy grows too fast, the Fed may raise interest rates as a means of ensuring price stability and protecting against inflation.

## Structure of the Federal Reserve

The chairman of the Federal Reserve leads a seven-member Board of Governors, all of whom are appointed by U.S. presidents. The president also appoints the chairman and vice-chairman from among the board members, appointments that must be confirmed by the U.S. Senate.

Alongside the board is another entity that arguably exerts as much power, the Federal Open Market Committee (FOMC), which oversees open market operations. The FOMC sets the objective for open market operations, meaning that it sets the federal funds rate. If the Fed purchases securities, thus adding to reserves, then depository institutions will tend to take on new loans and investments, which has the effect of lowering interest rates.

Of the seats on the FOMC, seven are filled by the members of the Board of Governors, and an eighth by the president of the New York Federal Reserve Bank. The other four are divided among the 11 other Federal Reserve banks, which fall into four groups (Boston, Philadelphia, and Richmond; Chicago and Cleveland; Atlanta, St. Louis, and Dallas; Minneapolis, Kansas City, and San Francisco), with presidents from each city in a group serving rotating one-year terms.

**Banks.** Although there are only 12 Federal Reserve banks, each has branches in other cities. For example, the Federal Reserve Bank of San Francisco has branches in Los Angeles, Portland, Seattle, and Salt Lake City. The 12 district banks release currency, and every banknote issued in the United States bears the seal of one of the district banks to the left of the portrait on the observe side.

Federal Reserve banks sell stock to member institutions, which include national and state-chartered banks, as well as trust companies. All national banks, which are chartered by the Office of the Comptroller of the Currency in the Treasury Department, automatically belong to the Fed, while state banks and trust companies have to meet requirements set by the Board of Governors. All members are required to purchase from their regional Federal Reserve banks stock equal to six percent of their capital, of which half is paid in, while the other half can be called in by the Board of Governors.

**Relationship with the federal government.** The Federal Reserve System is a part of the government in the sense that it was created by Congress, and is subject to congressional oversight. Furthermore, its leadership is appointed by presidents, although board members' 14-year terms extend far beyond the term of the chief executive who appointed them. Unlike most bureaus of the federal government, however, the Fed is independent of any cabinet-level department. Its decisions do not require the approval of the president, Congress, or any other member or body of the executive or legislative branches.

Nor does it depend on funding appropriated by Congress. Almost alone among government institutions, the Fed actually pays for itself through the interest it receives on its holdings of federal securities, and through the fees it charges depository institutions for such services as processing and clearing checks. As a non-profit institution, it turns its net earnings over to the Treasury each year. These earnings are far from inconsiderable: in 2001, the Federal Reserve paid \$27.14 billion to the federal government.

### ■ FURTHER READING:

#### BOOKS:

Greider, William. *Secrets of the Temple: How the Federal Reserve Runs the Country*. New York: Simon and Schuster, 1987.

Mayer, Martin. *The Fed: The Inside Story of How the World's Most Powerful Financial Institution Drives the Market*. New York: Free Press, 2001.

Woodward, Bob. *Maestro: Greenspan's Fed and the American Boom*. New York: Simon and Schuster, 2000.

#### ELECTRONIC:

Federal Reserve Board. <<http://www.federalreserve.gov/>> (February 5, 2003).

#### SEE ALSO

*Counterfeit Currency, Technology and the Manufacture IMF (International Monetary Fund) Treasury Department, United States*

---

## FEMA (United States Federal Emergency Management Agency)

---

Although today a component of the Department of Homeland Security (DHS), the Federal Emergency Management Agency (FEMA) is a formerly independent agency of





“Cowboy,” a search and rescue canine for the Federal Emergency Management Agency (FEMA), pauses during his work searching the World Trade Center site in New York in September, 2001. AP/WIDE WORLD PHOTOS.

the U.S. federal government tasked with responding to all aspects of natural and manmade disasters. This excludes specialized response capabilities such as those of radiological teams—although FEMA works with these—but includes all phases of disaster response, mitigation, and prevention. Created by a 1979 executive order, FEMA employs some 2,600 people at its headquarters in Washington, D.C., and at sites across the nation.

**Early history.** Federal efforts at disaster relief had their beginnings surprisingly early, in an 1803 congressional act authorizing assistance to a New Hampshire town ravaged by fire. Over the next century and a quarter, more than a hundred pieces of ad hoc legislation were passed in response to floods, hurricanes, earthquakes and other disasters.

The establishment of the Reconstruction Finance Program (RFP) under the New Deal of President Franklin D.

Roosevelt in the 1930s finally gave shape to federal disaster-relief efforts. The RFP, which made loans for repair and reconstruction in the wake of disasters, was soon augmented by the Bureau of Public Roads, which provided funding for the replacement of roads and bridges, and by the Flood Control Act, designed to enable the U.S. Army Corps of Engineers to implement flood control projects.

During the 1960s, a series of hurricanes lashed the United States, prompting the establishment of the Federal Disaster Assistance Administration within the Department of Housing and Urban Development. In 1968, Congress passed the National Flood Insurance Act, which increased the flood protection afforded to homeowners. The Disaster Relief Act of 1974 established the principle and process of disaster declarations on the part of the president, whose executive powers were sufficient to direct resources toward relief.

With more than 100 federal agencies involved in some aspect of disaster relief, the need for a coordinating agency became apparent, and in 1979 President James E. Carter issued an executive order creating FEMA. The new agency absorbed a number of entities, among them the Federal Preparedness Agency of the General Services Administration, HUD's Federal Disaster Assistance Administration, and the Defense Civil Preparedness Agency of the Department of Defense.

**FEMA today.** In its first quarter-century of existence, FEMA dealt with a vast array of natural and human disasters, including the nuclear accident at Three Mile Island in Pennsylvania in 1979, the Cuban refugee crisis in 1980, the San Francisco earthquake in 1989, Hurricane Andrew in 1992, floods in the Midwest and West in 1993, and the terrorist attacks of September 11, 2001.

The appointment of James L. Witt by President William J. Clinton in 1993 put FEMA for the first time under the leadership of a director with experience as a state emergency manager. Witt undertook wide-scale reforms that streamlined relief measures. Thanks to the end of the Cold War, he was also able to direct resources from civil defense toward disaster relief, as well as recovery and mitigation programs.

In the post-September 2001 era, a new type of "civil defense" emerged: homeland security. FEMA became part of DHS when the latter was formally established on March 1, 2003.

**Organization and mission.** In addition to its 2,600 full-time employees, FEMA has between 4,000 and 5,000 reservists. Its force operates out of FEMA headquarters; the FEMA training center at Emmitsburg, Maryland; the Mount Weather Emergency Operations Center in Virginia; and other facilities. FEMA often works in partnership with other groups, including some 27 federal agencies, state and local emergency management agencies, and the American Red Cross.

The mission and activities of FEMA relate to what the agency's own literature describes as the "life cycle of disaster." Starting with the disaster itself, there is the response phase, followed by recovery, mitigation, risk reduction, prevention, and preparedness—all of which makes the nation and its communities more equipped to deal with future catastrophes.

Among the specific activities FEMA undertakes are assisting with flood-plain management and implementation of building codes; teaching local communities how to survive a disaster; and equipping state and local emergency teams to prepare them for a disaster situation. In the event of a calamity, FEMA helps coordinate the federal response, and makes disaster assistance available to states, communities, businesses, and individuals. It also trains emergency managers, supports fire services nationwide, and administers national flood and crime insurance programs.

## ■ FURTHER READING:

### BOOKS:

Gore, Albert. *Federal Emergency Management Agency: Accompanying Report of the National Performance Review*. Washington, D.C.: Office of the Vice President, 1994.

Landesman, Linda Young. *Public Health Management of Disasters: The Practical Guide*. Washington, D.C.: American Public Health Association, 2001.

Therese, McAllister, and Gene Corley. *World Trade Center Building Performance Study: Data Collection, Preliminary Observations, and Recommendations*. Washington, D.C.: Federal Emergency Management Agency, 2002.

### PERIODICALS:

Adams, Shawn. "A Beginner's Guide to Learning Emergency Management." *Risk Management* 49, no. 5 (May 2002): 24–28.

"Reports Shed Light on World Trade Center Collapses, Look to Safer Structures in the Future." *JOM* 54, no. 6 (June 2002): 6.

Rubin, Debra K. "FEMA and Corps Plan New Guide for Terrorism Catastrophes." *ENR* 249, no. 15 (October 7, 2002): 14.

### ELECTRONIC:

Federal Emergency Management Agency. <<http://www.fema.gov>> (March 26, 2003).

### SEE ALSO

*Architecture and Structural Security*  
*Chemical Safety: Emergency Responses*  
*Homeland Security, United States Department*  
*Radiological Emergency Response Plan, United States Federal*

---

## FEST (United States Foreign Emergency Support Team)

---

The United States Foreign Emergency Support Team (FEST) is a rapid-response unit designed to respond to terrorist attacks against U.S. interests overseas. Created in 1985, it is directed by the Department of State, but constitutes an interagency force. Its most famous deployment occurred in 1998, when operatives of Osama bin Laden's al-Qaeda network bombed U.S. embassies in Kenya and Tanzania.

FEST was created to provide coordination and assistance to U.S. personnel and host nations in the event of an attack against American personnel and/or property overseas. Whenever deployed, it is directed by the chief of mission, who is the leading representative of the U.S.

president in a host nation (usually, but not always, this is an ambassador). Its efforts are coordinated by the Department of State, working through the Office of the Coordinator for Counterterrorism.

In crisis situations, FEST has the mission of advising, assisting, assessing, and coordinating. It provides the chief of mission, incident managers, and leaders of the host government with direction concerning Washington's response to a terrorist attack. FEST personnel are prepared to work around the clock in crisis and consequence management, communication augmentation, and other specialized tasks as directed. During the 1998 bombings in Africa, teams focused on restoring communications, ensuring security, and coordinating the flow of assistance to the embassies and personnel.

## ■ FURTHER READING:

### PERIODICALS:

Marcus, David L. "Horror at U.S. Embassies." *Boston Globe*. (August 8, 1998): A1.

Reiss, Tom. "Now Will We Heed the Biological Threat?" *New York Times*. (February 21, 1998): 11.

### ELECTRONIC:

Foreign Emergency Support Team. U.S. Department of State. <<http://www.state.gov/s/ct/rls/fs/2002/13045.htm>> (February 23, 2003).

### SEE ALSO

*Coordinator for Counterterrorism, United States Office Department of State, United States Domestic Emergency Support Team, United States Kenya, Bombing of United States Embassy*

## Fibalogy.

SEE *Stealth Technology*.

## Field Sieves Algorithms.

SEE *Cryptology and Number Theory*.

together with the valleys between them form unique patterns on the fingers. Fingerprint analysis is a biometric technique comparing scanned image of prints with a database of fingerprints. Uniqueness of prints, and the fact that they do not change during a person's life, form the basis for fingerprint analysis. The uniqueness of the prints is determined by the minute changes in local environment during fetal development; therefore, the identical twins undistinguishable by DNA analysis can be differentiated with fingerprint analysis. Although the fingerprint pattern remains the same, growth accounts for an enlargement of the patterns. Additionally, accidents or some diseases may alter fingerprint patterns

**History of fingerprint use.** Notes about the ridges, loops, and spirals of fingerprints were first made in 1686 by Marcello Malpighi. However, it was not until 1880 that fingerprints were recognized as a means of personal identification by Henry Faulds, who also identified a first ever fingerprint. The first book about fingerprints was published in 1888 by Sir Francis Galton, and was titled simply *Fingerprints*. Galton established the first classification system for fingerprints and was the first to assert that no two prints are the same, or that the odds of two prints being identical were about 1 in 64 billion. Later, the Henry Classification System was developed in 1901 by Sir Edward Henry, and today forms the basis for print recognition in most English speaking countries. This system categorized the ridge patterns into three groups: loops, whorls, and arches.

Fingerprinting was soon introduced in prisons, army and widely used for identification by law enforcement. The Federal Bureau of Investigation collection has millions of fingerprint cards and consists of approximately 70 million fingerprints. Although the main use of prints remains in forensic science and law enforcement, new uses of fingerprints have been developed.

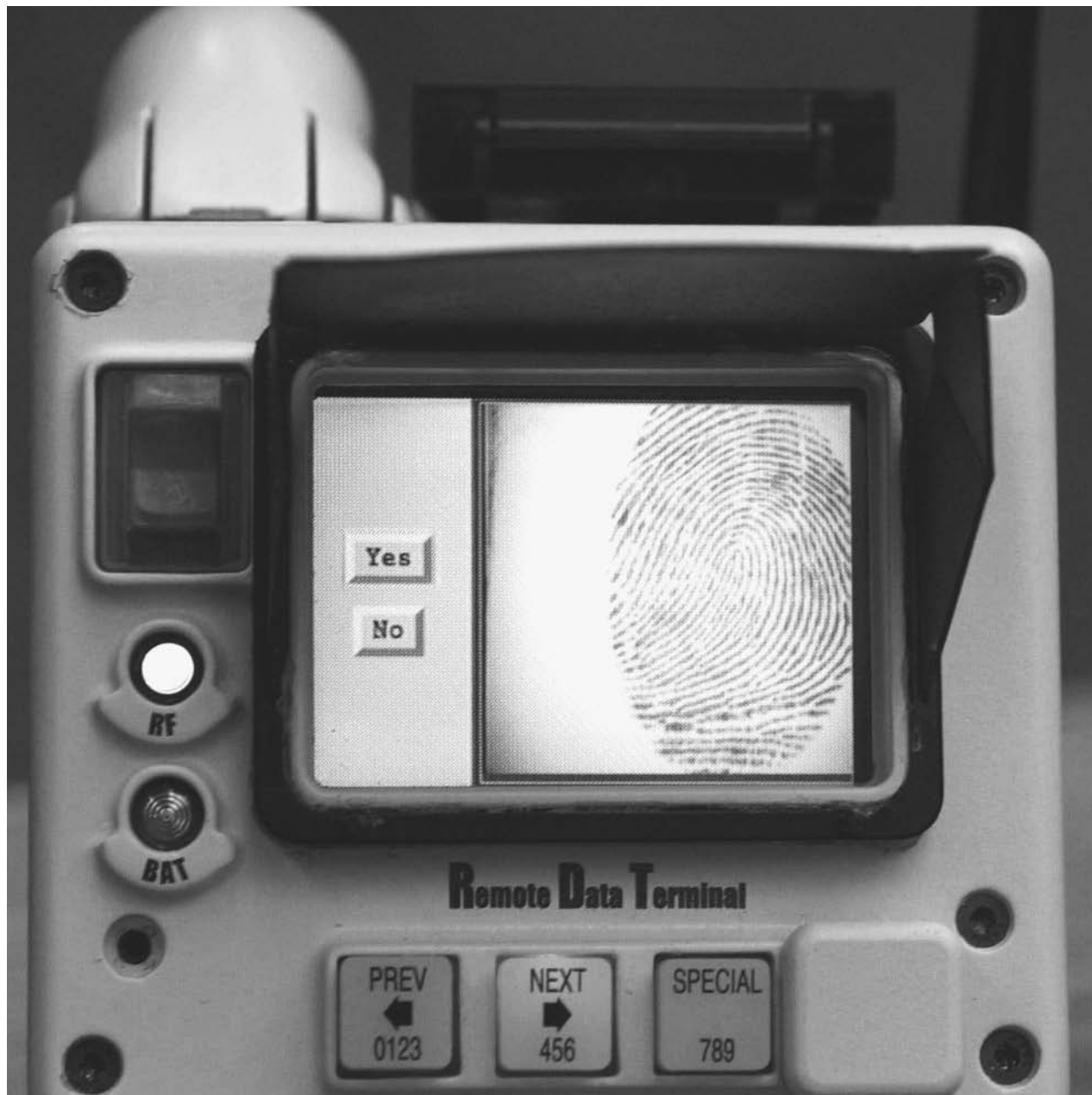
**Detection of fingerprints.** Presence of pores on the surface of the ridges of the fingers results in the accumulation of perspiration on the fingertips. This moisture remains on the surface of the object a person touches, leaving prints. Depending on the surface touched, prints can be visible to the naked eye (e.g. metal, glass or plastic) or invisible (paper, cardboard or timber). Prints left on non-porous surfaces such as metal can be visualized with powders and lifted with tape. In contrast, the prints on porous objects require special lighting, such as lasers or x rays.

There are two major methods of the identification of fingerprints—comparison of lifted prints and live scanning. The first method is mainly used in forensics, while the second is used for authentication purposes (in security applications) and is also slowly becoming a method for identification at some police stations.

# Fingerprint Analysis

## ■ AGNIESZKA LICHANSKA

Fingerprints are the patterns on the inside and the tips of fingers. The ridges of skin, also known as friction ridges,



A fingerprint is seen on the back of a wireless device called an "IBIS." It can record a fingerprint in the field, then send the fingerprint via a wireless connection to be checked against a database. AP/WIDE WORLD PHOTOS.

**Analysis and classification of fingerprints.** Ridges present on the fingers are classified based on the patterns they form. The most important features are ridge endings and bifurcations (separation of a ridge into two). These features are called minutiae and form the basis for further classification and identification. Based on the forms created by the minutiae (loops, whorls, etc.) fingerprints are further sub-classified into many more distinct patterns.

Modern fingerprint analysis uses computer algorithms to determine the similarity between a print and images

stored in a database. Analysis is usually performed on multiple levels. First, the algorithms are compared to the prints on the coarse level to identify a type of a print, and then subsequently to identify more and more details until a match is found. The computer analysis of prints compares ridges, bifurcations and their relative location. Fingerprint analysis software and scanners identify a set number of similarity points, this number being determined by the software used, typically up to 90 points are compared. After identification of a set number of features, a template of the scanned print is formed and this is

subsequently compared to the templates stored in the computer to determine if the print has a match. Although limiting the characteristics to be compared speeds up the matching process, it can also affect the accuracy if inadequate numbers are compared. Accuracy also depends on the application for which the fingerprint analysis is used.

Scanners have comparison algorithms and a number of recognizable characteristics programmed in, together with the prints of the users (enrolment) to provide the templates for comparison. The FBI fingerprint system is over 98% accurate, while the authentication systems accept only 97% of authorized users. Among some of the reasons for the rejection are: scars, calluses, cracks, dirt, or excess fingernail length.

**Fingerprint analysis tools.** Two types of fingerprint scanners are normally used, optical scanners and capacitance scanners. Optical scanners identify the print using light; depending on the brightness of the reflected light, optical scanners depict ridges as dark and valleys as light. Capacitance scanners determine the print by using an electrical current. Valleys and ridges on the fingers produce different voltage output, allowing for discrimination between them.

As sophisticated they are, the existing scanners are not totally immune to fraud. Optical scanners can be fooled by a picture, whereas the capacitance scanners can be fooled by a mold of a finger. Some scanners also have temperature and pulse sensors, but they are still vulnerable to molds placed over real fingers.

A number of portable fingerprint scanners were developed mainly by computer companies to provide a secure access for the users. In 1998, Compaq was the first to have a print reader attached to the computer. Currently, there are multiple systems for use with desktop and laptop computers in the form of PC cards and biometric mice. A portable print reader used for computer security employs a tiny digital camera to take a picture of a print and convert it into a map that is subsequently stored in the computer and cannot be duplicated.

Commercial fingerprint identification systems were introduced over 15 years ago. They are now used in security applications to gain access to a building or areas within the building, or computers or network access. Some companies, police offices, and high-security government buildings require fingerprint identification for access to the building or its selected parts.

In order to protect sensitive data, some businesses and the military often use scanners that are attached to computers (the U-Match mouse, for example) or installed in keyboards. These provide either immediate identification for access to the terminal or remote identification for access to secure documents or archives. NATO facilities in Turkey, and the U.S. Office of Legislative Council uses similar technology. New scanner trials are on the way to provide the same protection for e-commerce and Internet banking in order to secure transactions.

In order to combat cell phone thefts, the industry is considering equipping phones with fingerprint readers. Fingerprint protection is also offered for a new generation of safes, such as those provided by Biometrics Marketing. Finally, the scanners are being used to replace timecards in companies and to integrate payroll systems. Five U.S. airports, including Chicago's O'Hare have installed fingerprint scanners to check employees' backgrounds. Some banks use fingerprint scans before a check is cashed. Similarly, government agencies sometimes utilize fingerprint scans to ensure that payments are given to the proper recipients.

Today, fingerprint analysis technology is the most wide-spread biometric method of identification and authentication for forensic and security purposes.

#### ■ FURTHER READING:

##### BOOKS:

Ashbourn, Julian. *Advanced Identity Verification: The Complete Guide*. London: Springer Verlag, 2000.

Nanavati, Samir, Michael Thieme, and Raj Nanavati. *Biometrics: Identity Verification in a Networked World*. New York: Wiley and Sons, 2002.

##### ELECTRONIC:

Find Biometrics. <<http://www.findbiometrics.com/index.html>> (14 December 2002).

NCSC. "Individual biometrics." <<http://ctl.ncsc.dni.us/biomet%20web/BMFingerprint.html>> (14 December 2002).

##### SEE ALSO

*FBI (United States Federal Bureau of Investigation)*  
*Forensic Science*  
*Identity Theft*

---

## Finland, Intelligence and Security

---

Finland's geographic location made the nation one of the key strategic intelligence points during the twentieth century. Its position on the Baltic Sea, and proximity to both Russia and Western Europe, influenced the development of its national political character and intelligence community.

During World War II, as the Nazis planned their invasion of the Soviet Union and sought to stop operations of the Soviet Navy in the Baltic region, the Finnish government feared invasion. With the aid of the United States Office of Strategic Services, the forerunner of the Central

Intelligence Agency (CIA), members of Finland's intelligence community were smuggled into neighboring Sweden. The operation was known as Stella Polaris. There, agents sold the United States information on both Nazi Germany and the Soviet Union. However, Finnish intelligence also sold the same information to several other nations.

During the Cold War, Finland again was a key espionage and intelligence outpost. Both American and Soviet agents operated in Finland. Finland did not join the North Atlantic Treaty Organization (NATO), but provided western European and United States intelligence forces with crucial information on Soviet operations. As well, many Soviet defectors were smuggled through Finland.

Today, Finland maintains a few strategic intelligence services. Finnish intelligence's specialty is electronic and remote intelligence systems. As Finland is a member of the European Union (EU), its intelligence community is aiding the development of EU military intelligence.

In Finland, all intelligence services operate under the direction of the ministry of defense or the ministry of the interior. The national intelligence community makes the traditional distinction between internal and external intelligence, and divides its military and civilian agencies accordingly. Finnish military intelligence service is the General Staff Intelligence Division (PT). The agency is responsible for boarder control and foreign intelligence surveillance. Signals intelligence is gathered and processed at the agency's Communications Expertise Facility (VKL).

The civilian intelligence service, charged with domestic intelligence and internal security, is the Security Police (SUPO). The agency maintains extensive counter-espionage and counterintelligence units and aids development of security structures within the other national intelligence organizations. The agency maintains three operational divisions, the Unit of Development and Supportive activities, the Security Unit, and the Counter-espionage Unit.

In 2001, Finnish intelligence services began a two-year project to upgrade their existing electronic and remote surveillance equipment. Within the international community, Finnish intelligence pledged the use of this equipment to aid in global anti-terrorism efforts.

---

## First of October Anti-fascist Resistance Group (GRAPO)

---

The First of October Anti-fascist Resistance Group (GRAPO, or *Grupo de Resistencia Anti-Fascista Primero de Octubre*)

was formed in 1975 as the armed wing of the illegal Communist Party of Spain during the Franco era. Advocating the overthrow of the Spanish Government and replacement with a Marxist-Leninist regime, GRAPO is vehemently anti-U.S., calls for the removal of all U.S. military forces from Spanish territory, and has conducted and attempted several attacks against U.S. targets since 1977. The group issued a communiqué following the 11 September attacks in the United States, expressing its satisfaction that "symbols of imperialist power" were decimated and affirming that "the war" has only just begun. GRAPO has killed more than 90 persons and injured more than 200. The group's operations traditionally have been designed to cause material damage and gain publicity rather than inflict casualties, but the terrorists have conducted lethal bombings and close-range assassinations. In May, 2000, the group killed two security guards during a botched armed robbery attempt of an armored truck carrying an estimated \$2 million, and in November, 2000, members assassinated a Spanish policeman in a possible reprisal for the arrest that month of several GRAPO leaders in France. The group also has bombed business and official sites of the Madrid headquarters of the ruling Popular Party, including the Barcelona office of the national daily *El Mundo* in October 2000, when two police officers were injured.

Operating in Spain, GRAPO's exact strength is unknown, but likely has fewer than a dozen dedicated activists. Spanish and French officials have made periodic large-scale arrests of GRAPO members, crippling the organization and forcing it into lengthy rebuilding periods. The French and Spanish arrested several key leaders in 2001.

### ■ FURTHER READING:

#### ELECTRONIC:

- CDI (Center for Defense Information), Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <<http://www.cdi.org/terrorism/terrorist.cfm>> (April 17, 2003).
- Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).
- Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001," Annual Report: On the Record Briefing. May 21, 2002 <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17,2003).
- U.S. Department of State. Annual Reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

#### SEE ALSO

- Terrorism, Philosophical and Ideological Origins*
- Terrorist and Para-State Organizations*
- Terrorist Organization List, United States*
- Terrorist Organizations, Freezing of Assets*

## FISH (German *Geheimschreiber* Cipher Machine)

■ ADRIENNE WILMOTH LERNER

As late as the World War I era, cryptology depended on highly trained people at both ends of a communication to cipher and decipher a message. Codes were often kept in books that were vulnerable to enemy capture. The capturing of German code books by British military intelligence in World War I gave the Allies a significant tactical advantage. Soon after the war, technological advances in communication were applied to the sending and receiving of complexly coded text. Skilled cipherers and codebooks were replaced by cipher machines. Modern cryptographers, therefore, not only had to break enemy codes, but also determine how foreign cipher machines operated and generated codes. Cipher machines produced more mathematically intricate and random codes that were difficult to break. Because many cipher machine codes were dependent upon both the sender and the receiver machines, the capture of coded teleprinters did not dictate that a code could be broken.

In the 1930s, the German government commissioned the Seimans Company to create a cipher machine teleprinter that could produce, send, and receive plain and coded text. The idea behind the teleprinter was to randomize codes to make them more difficult to break, and to increase code information security. Seimans developed their first cipher teleprinter, the *Geheimschreiber*, with two encryption features, overlaying of code and transposition of pulses. Long pre-dating digital technology, both the basic encryption functions and the receipt of transpositioned pulses depended on mechanical circuits, namely various code wheels for text and charged capacitors and their corresponding relays for the pulse. The machine's ten code wheels had periods corresponding with prime numbers between 47 and 73. Thus, the wheels combined to form 893,622,318,929,520,960 permutations, or steps. Eight basic patterns with over two billion variations were possible in regards to pulse transposition. These combined encryption mechanisms led the German government to assume that the *Geheimschreiber* was nearly random and unbreakable; however, the mathematical patterns used by the machines proved to be more systematic than they perceived.

Teleprinters utilized the 32-character Baudot code. The code output consisted of five channels, represented as holes or no holes in varying orders, to produce each character. The German cipher machines relied on the Vernam cipher system, a mathematical code based on the principle of binary addition. That is, two coded characters were added together to produce the ciphered text. Code breakers knew of both the Baudot code and Vernam system, but the obscuring factors of the German *Geheimschreiber* made deciphering the code difficult.

The German cipher machines were supposed to change starting positions with every message, notifying the receiving end of a given transmission in plain text of the starting steps on the code wheels. Thus, the obscuring sequence of each code was supposedly unique. Code breakers in Sweden worked to break the *Geheimschreiber* code mathematically, and did so with measurable success in 1942. However, the work was tedious and by the time they had produced several decoding machines, the highest levels of the German command had begun to use the newer Lorenz cipher machine. Swedish cryptologists were unable to decipher any wire traffic after February, 1944.

British intelligence cryptologists at Bletchley Park thought the best hope of readily deciphering German teleprinters was to intercept a depth, or two messages that utilized the same starting position. While codebreakers had some success mathematically decoding Fish ciphered German transmissions, on August 30, 1941, British intelligence intercepted a 4,000-character-long depth. The Lorenz code was broken soon afterward by John Tiltman and Bill Tutte. Working out long code sequences by hand, the two uncovered the logical structure of the German cipher. With this knowledge, several "Tunny," now the code name for Lorenz transmissions, machines were constructed to facilitate decoding of intercepts. However, the start position settings of each message still had to be discovered by hand.

In 1943, British mathematician Max Newman and British engineer Tommy Flowers designed and built Colossus, a machine that not only simplified the process of deciphering German teleprinter intercepts, but that could be used with *Geheimschreiber*, Lorenz, and radio transmissions. Colossus' greatest contribution to codebreaking however was its ability to electronically decode the start position of each ciphered intercept, eliminating the need for painstaking hand calculations. The system was instrumental in the planning and execution of the allied D-Day invasion.

### ■ FURTHER READING:

#### BOOKS:

- Goldreich, Oded. *Foundations of Cryptography: Basic Tools*. Cambridge: Cambridge University Press, 2001.
- Hinsley, F. H. *British Intelligence in the Second World War*. Cambridge: Cambridge University Press, 1988.
- Hinsley, F. H. and Alan Stripp, eds. *Codebreakers: The Inside Story of Bletchley Park*. Oxford: Oxford University Press, 2001.
- Stinson, Douglas. *Cryptography: Theory and Practice*, second edition. Chapman and Hall, 2002.

#### SEE ALSO

*Bletchley Park*  
*Cipher Machines*  
*Colossus I*

---

## Fission

---

Nuclear fission is a process in which the nucleus of an atom splits, usually into two daughter nuclei, with the transformation of tremendous levels of nuclear energy into heat and light.

The fission reaction was discovered when a target of uranium was bombarded by neutrons. Fission fragments were shown to fly apart with a large release of energy. The fission reaction was the basis of the atomic bomb first developed by the United States during World War II. After the war, controlled energy release from fission was applied to the development of nuclear reactors. Reactors are utilized for production of electricity at nuclear power plants, for propulsion of ships and submarines, and for the creation of radioactive isotopes used in medicine and industry.

Long before the internal construction of the atom was well understood in terms of protons, neutrons, electrons, nuclear transformations that resulted in observable radioactivity were observed as early as 1896 by Henri French physicist Henri Becquerel (1852–1908). The fission reaction was first articulated by two German scientists, Otto Hahn (1879–1968) and Fritz Strassmann (1902–1980). In 1938, Hahn and Strassmann conducted a series of experiments in which they used neutrons to bombard various elements. Bombardment of copper, for example, produced a radioactive form of copper. Other elements became radioactive in the same way. When uranium was bombarded with neutrons, however, an entirely different reaction occurred. The uranium nucleus apparently underwent a major disruption. Accordingly, the initial evidence for the fission process came from chemical analysis. Hahn and Strassmann published a scientific paper showing that small amounts of barium (element 56) were produced when uranium (element 92) was bombarded with neutrons. Hahn and Strassmann questioned how a single neutron could transform element 92 into element 56.

Lise Meitner (1878–1968), a long-time colleague of Hahn who had left Germany due to Nazi persecution, suggested a helpful model for such a reaction. One can visualize the uranium nucleus to be like a liquid drop containing protons and neutrons. When an extra neutron enters, the drop begins to vibrate. If the vibration is violent enough, the drop can break into two pieces. Meitner named this process “fission” because it is similar to the process of cell division in biology. Moreover, it takes only a relatively small amount of energy to initiate nuclear instability.

Scientists in the United States and elsewhere quickly confirmed the idea of uranium fission, using other experimental procedures. For example, a cloud chamber is a device in which vapor trails of moving nuclear particles can be seen and photographed. In one experiment, a thin sheet of uranium was placed inside a cloud chamber.

When it was irradiated by neutrons, photographs showed a pair of tracks going in opposite directions from a common starting point in the uranium. Clearly, a nucleus had been photographed in the act of fission.

Another experimental procedure used a Geiger counter, which is a small, cylindrical tube that produces electrical pulses when a radioactive particle passes through it. For this experiment, the inside of a modified Geiger tube was lined with a thin layer of uranium. When a neutron source was brought near it, large voltage pulses were observed, much larger than from ordinary radioactivity. When the neutron source was taken away, the large pulses stopped. A Geiger tube without the uranium lining did not generate large pulses. Evidently, the large pulses were due to uranium fission fragments. The size of the pulses showed that the fragments had a very large amount of energy.

To understand the high energy released in uranium fission, scientists made some theoretical calculations based on German-American physicist Albert Einstein’s (1879–1955) famous equation  $E=mc^2$ . The Einstein equation states that mass  $m$  can be converted into energy  $E$  (and, conversely that energy can create mass). The conversion factor becomes  $c$ , the velocity of light squared. One can calculate that the total mass of the fission products remaining at the end of the reaction is slightly less than the mass of the uranium atom plus the neutron at the start. This decrease of mass, multiplied by  $c$ , shows numerically why the fission fragments are so energetic.

Through fission, neutrons of low energy can trigger a very large energy release. With the imminent threat of war in 1939, a number of scientists began to consider the possibility that a new and very powerful “atomic bomb” could be built from uranium. Also, they speculated that uranium perhaps could be harnessed to replace coal or oil as a fuel for industrial power plants.

Nuclear reactions in general are much more powerful than chemical reactions. A chemical change such as burning coal or even exploding TNT affects only the outer electrons of an atom. A nuclear process, on the other hand, causes changes among the protons and neutrons inside the nucleus. The energy of attraction between protons and neutrons is about a million times greater than the chemical binding energy between atoms. Therefore, a single fission bomb, using nuclear energy, might destroy a whole city. Alternatively, nuclear electric power plants theoretically could run for a whole year on just a few tons of fuel.

In order to release a substantial amount of energy, many millions of uranium nuclei must split apart. The fission process itself provides a mechanism for creating a so-called chain reaction. In addition to the two main fragments, each fission event produces two or three extra neutrons. Some of these can enter nearby uranium nuclei and cause them in turn to fission, releasing more neutrons, which causes more fission, and so forth. In a bomb



explosion, neutrons have to increase very rapidly, in a fraction of a second. In a controlled reactor, however, the neutron population has to be kept in a steady state. Excess neutrons must be removed by some type of absorber material (e.g., neutron absorbing control rods).

In 1942, the first nuclear reactor with a self-sustaining chain reaction was built in the United States. The principal designer was Enrico Fermi (1901–1954), an Italian physicist and the 1938 Nobel Prize winner in physics. Fermi emigrated to the United States to escape Benito Mussolini's fascism. Fermi's reactor design had three main components: lumps of uranium (the fuel), blocks of carbon (the moderator, which slows down the neutrons), and control rods made of cadmium (an excellent neutron absorber). Fermi and other scientists constructed the first nuclear reactor pile at the University of Chicago. When the pile of uranium and carbon blocks was about 10 ft (3 m) high and the cadmium control rods were pulled out far enough, Geiger counters showed that a steady-state chain reaction had been successfully accomplished. The power output was only about 200 watts, but it was enough to verify the basic principle of reactor operation. The power level of the chain reaction could be varied by moving the control rods in or out.

General Leslie R. Groves was put in charge of the project to convert the chain reaction experiment into a usable military weapon. Three major laboratories were built under wartime conditions of urgency and secrecy. Oak Ridge, Tennessee, became the site for purifying and separating uranium into bomb-grade material. At Hanford, Washington, four large reactors were built to produce another possible bomb material, plutonium. At Los Alamos, New Mexico, the actual work of bomb design was started in 1943 under the leadership of the physicist J. Robert Oppenheimer (1904–1967).

The fissionable uranium isotope, uranium-235, constitutes only about 1% of natural uranium, while the non-fissionable neutron absorber, uranium-238, makes up the other 99%. To produce bomb-grade, fissionable uranium-235, it was necessary to build a large isotope separation facility. Since the plant would require much electricity, the site was chosen to be in the region of the Tennessee Valley Authority (TVA). The technology of large-scale isotope separation involved solving many difficult, unprecedented problems. By early 1945, the Oak Ridge Laboratory was able to produce kilogram amounts of uranium-235 purified to better than 95%.

An alternate possible fuel for a fission bomb is plutonium-239. Plutonium does not exist in nature but results from radioactive decay of uranium-239. Fermi's chain reaction experiment had shown that uranium-239 could be made in a reactor. However, to produce several hundred kilograms of plutonium required a large increase from the power level of Fermi's original experiment. Plutonium production reactors were constructed at Hanford, Washington, located near the Columbia River to provide needed cooling water. A difficult technical problem was

how to separate plutonium from the highly radioactive fuel rods after irradiation. This was accomplished by means of remote handling apparatus that was manipulated by technicians working behind thick protective glass windows.

With uranium-235 separation started at Oak Ridge and plutonium-239 production under way at Hanford, a third laboratory was set up at Los Alamos, New Mexico, to work on bomb design. In order to create an explosion, many nuclei would have to fission almost simultaneously. The key concept was to bring together several pieces of fissionable material into a so-called critical mass. In one design, two pieces of uranium-235 were shot toward each other from opposite ends of a cylindrical tube. A second design used a spherical shell of plutonium-239, to be detonated by an "implosion" toward the center of the sphere.

The first atomic bomb was tested at an isolated desert location in New Mexico on July 16, 1945. President Truman then issued an ultimatum to Japan that a powerful new weapon could soon be used against them. On August 8, a single U.S. atomic bomb destroyed the city of Hiroshima with over 80,000 casualties. On August 11, a second bomb was dropped on Nagasaki with a similar result. Japan surrendered three days later to end WWII.

The possibility of a terrorist group or a dictator hostile to Western democracies obtaining nuclear weapons is a continuing threat to world peace. In late 2001, in the aftermath of the terrorist attacks on the World Trade Center in New York, intelligence agencies released evidence of terrorist attempts to acquire weapons grade uranium and the other technology related to bomb production.

The first nuclear reactor designed for producing electricity was put into operation in 1957 at Shippingsport, Pennsylvania. From 1960 to 1990, more than 100 nuclear power plants were built in the United States. These plants now generate about 20% of the nation's electric power. World-wide, there are over 400 nuclear power stations.

The most common reactor type is the pressurized water reactor (abbreviated PWR). The system operates like a coal-burning power plant, except that the firebox of the coal plant is replaced by a reactor. Nuclear energy from uranium is released in the two fission fragments. The fuel rod becomes very hot because of the cumulative energy of fissioning nuclei. A typical reactor core contains hundreds of these fuel rods. Water is circulated through the core to remove the heat. The hot water is prevented from boiling by keeping the system under pressure (i.e., creating superheated steam).

The pressurized hot water goes to a heat exchanger where steam is produced. The steam then goes to a turbine, which has a series of fan blades that rotate rapidly when hit by the steam. The turbine is connected to the rotor of an electric generator. Its output goes to cross-country transmission lines that supply the electrical users in the region. The steam that made the turbine rotate is

condensed back into water and is recycled to the heat exchanger.

Safety features at a nuclear power plant include automatic shutdown of the fission process by insertion of control rods, emergency water-cooling for the core in case of pipeline breakage, and a concrete containment shell. It is impossible for a reactor to have a nuclear explosion because the fuel enrichment in a reactor is intentionally limited to about 3% uranium-235, while almost 100% pure uranium-235 is required for a bomb. Regardless, nuclear power plants remain potential targets for terrorists who would seek to cause massive and lethal release of radioactivity by compromising the containment shell.

The fuel in the reactor core consists of several tons of uranium. As the reactor is operated, the uranium content gradually decreases because of fission, and the radioactive waste products (the fission fragments) build up. After about a year of operation, the reactor must be shut down for refueling. The old fuel rods are pulled out and replaced. These fuel rods, which are very radioactive, are stored under water at the power plant site. After five to ten years, much of their radioactivity has decayed. Only those materials with a long radioactive lifetime remain, and eventually they must be stored in a suitable underground depository.

There are vehement arguments for and against nuclear power. As with other forms of electricity production, nuclear power generation can have serious and unintended environmental impacts. The main objections to nuclear power plants are the fear of possible accidents, the unresolved problem of nuclear waste storage, and the possibility of plutonium diversion for weapons production by a terrorist group. The issue of waste storage becomes particularly emotional because leakage from a waste depository could contaminate ground water. Opponents of nuclear power often cite accidents at the Three Mile Island nuclear power plant in United States and the massive leak at the Chernobyl nuclear plant in the USSR (now the Ukraine) as evidence that engineering or technical failures can have long lasting and devastating environmental and public health consequences.

The main advantage of nuclear power plants is that they do not cause atmospheric pollution. No smokestacks are needed because nothing is being burned. France initiated a large-scale nuclear program after the Arab oil embargo in 1973 and has been able to reduce its acid rain and carbon dioxide emissions by more than 40%. Nuclear power plants do not contribute to potential global warming. Shipments of fuel are minimal and so the hazards of coal transportation and oil spills are avoided.

#### ■ FURTHER READING:

##### BOOKS:

Cottingham, W. Noel and Derek A. Greenwood. *An Introduction to the Standard Model of Particle Physics*. New York: Cambridge University Press, 1999.

Sagan, Scott D. and Kenneth N. Waltz. *The Spread of Nuclear Weapons: A Debate Renewed*, Second Edition. New York: W W Norton & Co., 2003.

Whiting, Jim. *Otto Hahn and the Story of Nuclear Fission*. Childs. MD: Mitchell Lane Publishers, Inc. 2003.

##### PERIODICALS:

Ladika, Susan. "Tracing the Shadowy Origins of Nuclear Contraband." *Science* no. 5522 (2001): 1634.

##### ELECTRONIC:

United States Department of Energy. "Guide to the Nuclear Wallchart: Energy From Nuclear Science" (August 2000) <<http://www.nsd.lbl.gov/abc/wallchart/chapters/14/0.html>> (March 20, 2003).

##### SEE ALSO

*Fusion*  
*Heavy Water Technology*  
*Manhattan Project*  
*Nuclear Detection Devices*  
*Nuclear Emergency Support Team, United States*  
*Nuclear Power Plants, Security*  
*Nuclear Reactors*  
*Nuclear Regulatory Commission (NRC), United States*  
*Nuclear Spectroscopy*  
*Nuclear Weapons*  
*Oak Ridge National Laboratory (ORNL)*  
*Weapon-Grade Plutonium and Uranium, Tracking*

---

## Flame Analysis

---

Flame tests are useful means of determining the composition of substances. The colors produced by the flame test are compared to known standards. And the presence of certain elements in the sample can be confirmed. The color of the flame and its spectrum (component colors) is unique for each element.

Flame analysis or atomic emission spectroscopy (AES) is based on the physical and chemical principle that atoms—after being heated by flame—return to their normal energy state by giving off the excess energy in the form of light. The frequencies of the light given off are characteristic for each element.

Flame analysis is a qualitative test and not a quantitative test. A qualitative chemical analysis is designed to identify the components of a substance or mixture. Quantitative tests measure the amounts or proportions of the components in a reaction or substance.

The unknown to be subjected to flame analysis is either sprayed into the flame or placed on a thin wire that is then put into the flame. Volatile elements (chlorides) produce intense colors. The yellow color of sodium, for example, can be so intense that it overwhelms other

colors. To prevent this the wire to be coated with the unknown sample is usually dipped in hydrochloric acid and subjected to flame to remove the volatile impurities and sodium.

The flame test does not work on all elements. Those that produce a measurable spectrum when subjected to flame include, but are not limited to, lithium, sodium, potassium, rubidium, cesium, magnesium, calcium, strontium, barium, zinc, and cadmium. Other elements may need hotter flames to produce measurable spectra.

Special techniques are required to properly interpret the results of flame analysis. The colors produced by a potassium flame (pale violet) can usually be observed only with the assistance of glass that can filter out interfering colors. Some colors are similar enough that line spectrum must be examined to make a complete and accurate identification of the unknown substance, or the presence of an identifiable substance in the unknown.

Flame analysis can also be used to determine the presence of metal elements in water by measuring the spectrum produced by the metals exposed to flame. The water is vaporized and then the emissions of the vaporized metals can be analyzed.

#### ■ FURTHER READING :

##### BOOKS:

Broekaert, José. C. *Analytic Atomic Spectrometry with Flames and Plasmas*. New York: Wiley-VCH Publishing, 2001.

##### ELECTRONIC:

Helmenstein, Anne Marie. "What You Need To Know About Chemistry-Quantitative Flame Analysis" About, Inc, <<http://chemistry.about.com/library/weekly/aa110401a.htm>> (March 29, 2003).

##### SEE ALSO

*Air and Water Purification, Security Issues  
Chemical and Biological Detection Technologies  
Isotopic Analysis  
Spectroscopy  
Water Supply: Counter-Terrorism*

## Flash X-Ray Facility.

SEE *Lawrence Livermore National Laboratory (LLNL)*.

## Flight Data Recorders

■ KELLI A. MILLER

In the earliest days of air transportation, plane crashes yielded few clues for safety investigators. Investigators



The charred casing of the flight data recorder recovered from the crash of American Airlines flight 587 is displayed at the National Transportation Safety Board in 2001, along with a normal, undamaged flight recorder (at rear). AP/WIDE WORLD PHOTOS.

would struggle to figure out what happened immediately preceding the accident but often fail to come to any definite conclusions regarding the cause of the crash. In June 1960, a Fokker F27 plane crashed while landing in Queensland, Australia, killing 29 people. Despite intensive investigations, the underlying cause for the accident was never determined. The mystery prompted the Australia board of inquiry to recommend that all airplanes be fitted with a flight data recorder (FDR) that would detail the flight crew's conversation.

Efforts to make the FDR a mandatory part of civil aircraft date back to the early 1940s. The idea, however, was wrought with one enormous technological challenge. Design specifications required that the unit survive the forces of an aircraft crash, as well as any resulting fire exposure.

In 1953, at a time when flight engineers were attempting to understand why a number of airliners had inexplicably crashed, Australian aviation scientist David Warren of the Aeronautical Research Laboratories in Melbourne invented a fully automatic "Flight Memory Unit." His prototype could record cockpit noise and instrument readings and remain in tact following a crash or fire. Much to Warren's surprise, Australian aviation experts and pilots originally rejected the idea, on the premise of privacy

issues. Warren took the concept to the United Kingdom, where it was well received by aviation officials. By 1957, the FDR was in production. Australia was among the first countries to require the device on commercial aircraft.

The phrase “black box,” however, is a misnomer. Flight data recorders are actually painted a bright red or orange for easier location after a crash. The FDR is encased in heavy steel and surrounded by multiple layers of insulation to provide protection against a crash, fire, and extreme climatic conditions. The device records actual flight conditions, including altitude, airspeed, heading, vertical acceleration and aircraft pitch. A second device, the cockpit voice recorder (CVR), keeps tabs on cockpit conversations and engine noise. Both are installed in the rear of the aircraft.

In the 1970s, FDR technology was combined with a flight-data acquisition unit (FDAU), located at the front of the aircraft. The unit acts as the relay for the entire data-recording process. Sensors run from various areas on the plane to the FDAU, which in turn sends the information to the FDR.

In the early days, data were embossed onto a type of magnetic foil known as Incanol Steel. The foil proved to be destructible and FDR manufacturers began using a more reliable form of magnetic tape. Electromagnetic technology remained the data-recording medium of choice until the late 1990s, when solid-state electronics began to show promise. Solid-state recorders rely on stacked arrays of non-moveable memory chips. The technology is considered more reliable than magnetic tape, as the lack of moving parts provides a reduced chance of breakage during a crash.

Solid-state recorders also track a much greater number of parameters; 700 are tracked compared to the magnetic tape parameter recording potential of 100. Faster data flow allows the solid-state devices to record up to 25 hours of flight data. In 1997, the United States Federal Aviation Administration (FAA) issued a requirement that all aircraft manufactured after August 19, 2002 record at least 88 parameters. The action came in the wake of two B-737 airplane crashes in which insufficient data was available for determining the cause of the accidents.

In addition to the five above-mentioned parameters recorded by the earliest data recorders, today’s devices also track time, control-column position, rudder-pedal position, control-wheel position, horizontal stabilizer, and fuel flow.

Since its inception, the FDR has played a vital role in establishing the probable cause of a crash or other unusual occurrences and has allowed safety regulators to implement corrective actions. The value of flight data recorders was clearly evident in the investigation of the ATR-72 accident in Roselawn, Indiana in October 1994. The FDR captured information on 115 parameters. Analysis of the data revealed a telltale, rapid wing movement that prompted the National Transportation and Safety

Board to immediately issue urgent safety recommendations to improve flying in icing conditions.

## ■ FURTHER READING:

### ELECTRONIC:

“The Black Box: An Australian Contribution to Air Safety,” March 21, 2002 <<http://www.dsto.defence.gov.au/corporate/history/jubilee/blackbox.html>>(December 08, 2002).

“Black Boxes,” February 22, 2002 <<http://www.atsb.gov.au/aviation/editorial/flrec/index.cfm>>(December 08, 2002).

“A History of the Black Box,” <<http://www.millennium.scps.k12.fl.us/istfbbhistory.html>>(December 08, 2002).

“How Things Work: Black Boxes,” <<http://www.howstuffworks.com/black-box1.htm>>(December 08, 2002).

L-3 Communications Corp., “Aviation Recorders,” 2002, <<http://www.l-3ar.com/html/history.html>> (December 11, 2002).

National Transportation and Safety Board, “Data Collection and Improved Technologies,” May 20, 1998 <<http://www.nts.gov/speeches/s980520.htm>> (December 08, 2002).

### SEE ALSO

*FAA (United States Federal Aviation Administration)*  
*NTSB (National Transportation Safety Board)*  
*Shoe Transmitter*  
*Short-Wave Transmitters*

---

## FM Transmitters

---

FM (frequency modulation) transmitters can yield a number of results, depending on their power and range. Extremely low-power transmitters can be used in very small locales, for purposes such as eavesdropping. At the high end, radio transmitters are sometimes used for propaganda and psychological warfare through broadcasting. Between these extremes are the low-power radio transmitters, capable of making every user a broadcaster, that have long been an issue of concern for the Federal Communications Commission (FCC).

Mini transmitters, which have a range of about 50 feet (15.2 m), are available commercially to serve purposes such as that of a baby monitor, but are easily adapted for eavesdropping as well. Although they are capable of operating anywhere on the FM dial, from 88 to 108 MHz, the recommended range for most of these is 88 to 95 MHz, where there is least likely to be interference. Low-power FM transmitters, with a range of 100 to 400 feet (30.5–122 m), make it possible to transmit voices over a greater distance, and are applied commercially for purposes such as listening to compact discs (CDs) in a car that does not have a CD player.

Both mini and low-power FM transmitters have such limited power—less than 1 watt—that they pose no concern to communications regulators. On the other hand, high-power or professional FM transmitters that are commercially available—some with as many as 35 watts of power—theoretically have the capacity to make anyone a radio broadcaster. This could pose serious concerns with regard to interference and communication jamming, and by 1998, the availability of FM transmitters forced the FCC to at least consider the idea of legalizing low-power transmission. The concept has been under consideration for some time, but many would-be broadcasters are as likely to choose the Internet as a simpler, non-interfering environment in which to operate a radio site.

In the realm of very high-power radio stations, there are many such facilities overseas operated by the federal government for the purposes of winning over local populations. In February, 2002, a year before the administration of President George W. Bush launched Operation Iraqi Freedom, it provided assistance to the opposition Iraqi National Congress as it began transmitting from the Kurdish-dominated north of Iraq on the FM dial. The United States already broadcast on short-wave radio into Iraq, but FM is both more popular and harder to jam than short-wave or AM (ampere modulation).

#### ■ FURTHER READING :

##### PERIODICALS:

- Braga, Newton C. "Experimenting with Small FM Transmitters." *Poptronics 2*, no. 9 (September 2001): 41–46.
- Gordon, Michael R. "Radio Transmitter to Oppose Hussein Wins U.S. Support." *New York Times*. (February 28, 2002): A1.
- "Low-Power FM Transmitters." *Electronics Now 70*, no. 8 (August 1999): 37–40.
- Schneider, Howard. "A Little U.S. Pop-aganda for Arabs." *Washington Post*. (July 26, 2002): A24.
- Schweber, Bill. "FM Transmitter/Receiver Provides 433-MHz Link." *EDN 47*, no. 9 (April 18, 2002): 22.

##### SEE ALSO

*FCC (United States Federal Communications Commission) Iraqi Freedom, Operation (2003 War Against Iraq)*  
*National Telecommunications Information Administration, and Security for the Radio Frequency Spectrum, United States*  
*Shoe Transmitter*  
*Short-Wave Transmitters*

## FOIA (Freedom of Information Act)

The Freedom of Information Act (FOIA) limits the ability of United States federal government agencies to withhold



Kate Martin, shown in her office at the Center for National Security Studies of George Washington University's Gelman Library. She was a lead attorney in a Freedom of Information Act case seeking the disclosure of the identities of hundreds of individuals who were arrested and jailed after the September 11 terrorist attacks. AP/WIDE WORLD PHOTOS.

information from the public by classifying that information as secret. Passed by Congress in 1967, it applies to the agencies of the executive branch, and not to the legislative or judicial branches, or to state or local governments, although every state has its own privacy and public access laws. FOIA did not become a significant aspect of American public life until the early to mid-1970s, when several events, including the Watergate scandal, the passage of the Privacy Act in 1974, and amendments in 1975, helped give it much greater importance.

### Historical Background

When Congress first passed FOIA, the law did not apply to investigatory files compiled for the purposes of law enforcement. This exempted files collected by the Justice Department and its agencies, most notably the Federal Bureau of Investigation (FBI), from the FOIA. Within a few years of the law's passage, however, the fabric of American public life would change dramatically, bringing with it changes in many of the nation's laws, including FOIA.

Whereas ordinary citizens had long been accustomed to trusting their government and to respecting organizations such as the FBI and Central Intelligence Agency (CIA), revelations of spying and other “dirty tricks” committed by the Nixon administration before and during the Watergate years helped influence a sense of distrust of Washington. Prior to the early 1970s, suspicion of the federal government was limited primarily to those on the political fringes of right and left, but thereafter, the belief that the government was spying on its citizens became an increasingly prevalent attitude.

**The Privacy Act and changes to the FOIA.** By the mid-1970s, this change in attitude would be reflected in Washington by efforts to increase the openness of the federal government to its citizens. Nixon himself issued an executive order limiting the number of agencies that could classify information as top secret, and thus exempt it from FOIA provisions. He also required officials in such situations to explain why information had been classified as top secret in the first place.

The scandal surrounding Watergate, and the looming possibility of an impeachment, forced Nixon’s resignation in 1974, the same year Congress passed the Privacy Act. The latter greatly restricted the authority of agencies to collect information on individuals, and to disclose that information to persons other than the individual. At the same time, it required the agencies to furnish the individual with any information on him or her that the agency had in its files. The Privacy Act, along with 1975 amendments to FOIA, greatly broadened access to federal files—including those of law-enforcement, intelligence, and security agencies—that had formerly been under severe restriction.

**FOIA procedure today.** In addition to restricting the purview of federal agencies with regard to documents, what came to be known as the Freedom of Information-Privacy Acts (FOIPA) placed an enormous onus on those agencies to respond to all requests for information. For example, in the quarter-century after 1975, the FBI handled some 300,000 requests involving the release of more than 6 million pages of documents. Not every part of every request is granted, however: FOIPA does allow exemptions for sensitive material.

In some situations, the requester has to pay for fulfillment of the request. Answers to questions regarding payment and any number of other specifics may be found with the Department of Justice, which in 2003 maintained an FOIA section at its Web site. There it listed FOIA contacts at various government agencies, as well as other information relating to FOIPA.

By the early twenty-first century, every federal department, agency, office, and bureau had its own FOIA contact. For most entities of any size, there was at least

one individual tasked full-time with processing, responding to, and fulfilling these requests. In some cases, there were multiple individuals or even an entire office devoted to this purpose.

At the FBI, for instance, requests are received, logged into computers, and assigned a tracking number. The agency then formally acknowledges the request, and conducts an indices search to determine whether it even has the records requested. Once an apparent match is located, it is reviewed to determine whether it is the exact file requested.

Assuming the file exactly matches the request, it is photocopied, and an analyst reviews the work copy to determine if there is any material that meets any one of nine exemptions and three exclusions covered in FOIPA. If any such material exists in the file, the analyst uses a colored marker to delete it, and in the margins cites the appropriate exemption. The pages are then re-copied using a photocopier with a special filter so that there is no chance anyone can detect the deleted material. At that point, the copies are mailed to the requester.

During the early twenty-first century, the FBI and other agencies were developing automated document processing systems that would replace many of these steps. These systems would also remove the need for a marker pen, and would allow for documents to be released in electronic format.

## ■ FURTHER READING:

### BOOKS:

- Henderson, Harry. *Privacy in the Information Age*. New York: Facts on File, 1999.
- Sherick, L. G. *How to Use the Freedom of Information Act (FOIA)*. New York: Arco, 1978.
- Theoharis, Athan G. *A Culture of Secrecy: The Government Versus the People’s Right to Know*. Lawrence: University of Kansas Press, 1998.
- Ullmann, John, and Steve Honeyman. *The Reporter’s Handbook: An Investigator’s Guide to Documents and Techniques*. New York: St. Martin’s Press, 1983.

### ELECTRONIC:

- Freedom of Information Act (FOIA). U.S. Department of Justice. <<http://www.usdoj.gov/04foia/>> (March 16, 2003).

### SEE ALSO

- CIA, Legal Restriction Classified Information*
- FBI (United States Federal Bureau of Investigation)*
- Intelligence, United States Congressional Oversight*
- Justice Department, United States*
- Nixon Administration (1969–1974), United States National Security Policy*
- Privacy: Legal and Ethical Issues*
- Security Clearance Investigations*
- Watergate*

## Food Supply, Counter-Terrorism

■ BRIAN HOYLE

The 1995 release of Sarin gas in the Tokyo subway system, and the events of September 11, 2001 in the United States illustrate society's vulnerability to terrorist attack in the course of everyday activities. Much of the infrastructure of public life (i.e., buildings, subways, airports) was not initially designed to thwart malicious activity. Food supplies are an additional component of the infrastructure, and as such, are also vulnerable to terrorism. Crops in the field are relatively unprotected. Food that is processed is monitored, not to detect the deliberate addition of a poison or an infectious agent, but to verify that the product is free from a small number of bacterial contaminants. Finally, on the supermarket shelf, products can be altered.

Terrorist attacks on a nation's food supply could not only cause illness, but also can cripple an economy. For example, the agricultural sector in the U.S. accounts for 13% of the country's gross domestic product and provides jobs for about 40 million Americans.

A disease outbreak carries the potential to cripple an economy. One example is the 1997 outbreak of Foot and Mouth disease among herds of pork in Taiwan. Battling the outbreak cost \$7 billion. A similar outbreak in Britain in 2001 drained well over \$4 billion from the economy.

**The threats to food supplies.** Obtaining a strain of bacteria or virus that causes plant or animal diseases is much easier than obtaining a highly infectious human pathogen. Agricultural pathogens can even be obtained from the environment. For example, scraping the surface of infected leaves is sufficient to recover some disease-causing viruses. Both the former Soviet Union and Iraq are known to have experimented with agricultural pathogens. Thus, a terrorist group having some microbiological expertise could acquire the microorganisms needed for their attacks.

Microorganisms can also be purchased from supply laboratories. An organization with convincing paperwork would be able to acquire microbes that are not considered to be highly infectious.

The advent of recombinant DNA technology in the 1970s—where a segment of genetic material coding for a protein of interest (i.e., a toxin) can be isolated and spliced into the DNA of a target microbe—holds the potential for the genetic modification of bacteria or viruses that are common in the environment. These genetic versions could spread quickly through the natural world.

**Counter-terrorism measures.** Following the September 11, 2001 terrorist attacks, the U.S. government moved to

strengthen the country's defense against bioterrorism. This initiative culminated in the signing into law, on June 12, 2002, of the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (the Bioterrorism Act). The act authorized the secretary of Health and Human Services to protect the nation's food supply. The U.S. Food and Drug Administration (FDA) is the lead agency in initiating the protective measures.

The U.S. measures are aimed at providing a system of accountability. For example, all businesses or growers who sell food for consumption in the U.S. must register with the government. As well, these firms will be required to maintain records of their food handling and processing activities. In the event of a deliberate contamination, this information would allow the source of the contamination to be traced.

The surveillance of food also must include inspection of food entering the country. This involves the manual inspection of foods arriving by air, sea, rail, and surface routes. As of 2003, these inspections typically consist of the visual examination of foods, although the use of portable devices that detect microorganisms or their products is being used experimentally. Other such devices are in the laboratory stage of testing, and have produced accurate results in laboratory settings.

Because protection of a nation's food supply cannot be absolute, a system of early warning of a bioterrorist attack is important. If widespread alerts are recognized soon enough, relatively few people will have consumed the contaminated food. Consumer vigilance is an additional important counter-terrorism measure. For example, even if raw produce has been doused with a poison or an infectious microorganism, careful washing will usually remove the threat. Canned foods that are damaged or swollen should be identified and discarded.

### ■ FURTHER READING:

#### BOOKS:

Layton, Peggy Diane. *Emergency Food Storage & Survival Handbook: Everything You Need to Know to Keep Your Family Safe in a Crisis*. Roseville, CA: Prima Publishing, 2002.

Pottier, John. *Anthropology of Food: The Social Dynamics of Food Security*. Oxford: Polity Pr., 1999.

#### PERIODICALS:

Turco, R.P., A.B. Toon, T.P. Ackerman, et al. "Nuclear Winter: Global Consequences of Multiple Nuclear Explosions." *Science* no. 222 (1983): 1283–1297.

#### ELECTRONIC:

Purdue University. "Agoterrorism." Purdue Extension Backgrounder. September 24, 2001. <<http://www.ces.purdue.edu/eden/disasters/agro/Agroterrorism.doc>>(24 January 2003).

United States Food and Drug Administration. "Frequently Asked Consumer Questions About Food Safety and

Terrorism." Center for Food Safety and Applied Nutrition. January 16, 2002. <<http://vm.cfsan.fda.gov/~dms/fsterrqu.html>>(23 January 2003).

———. "Protecting the Food Supply: FDA Actions on New Bioterrorism Legislation." Center for Food Safety and Applied Nutrition. November 18, 2002. <<http://www.cfsan.fda.gov/~dms/fsbtact3.html>>(24 January 2003).

#### SEE ALSO

*Biosensor Technologies*

*Microbiology: Applications to Espionage, Intelligence and Security*

*Polymerase Chain Reaction (PCR)*

*Salmonella and Salmonella Food Poisoning*

## Ford Administration (1974–1977), United States National Security Policy

■ CARYN E. NEUMANN

When Gerald Ford assumed the presidency of the United States upon the 1974 resignation of Richard Nixon, he chose to continue most of Nixon's national security policy. Secretary of State Henry Kissinger remained in office as the principal manager of national security matters while détente with the Soviet Union continued as a chief U.S. goal. The two administrations differed in that Ford never enjoyed Nixon's foreign policy successes. The Ford administration's accomplishments in arms control were overshadowed by the loss of South Vietnam to the Communists as well as doubts about the enforceability of the Vladivostok arms agreement.

A cautious mainstream Republican from Michigan who had served for many years as the minority leader in the U.S. House of Representatives, the amiable Ford came to the White House at an inauspicious time. Some Americans had lost faith in political leaders, largely as a result of the Watergate scandal, and this change made it difficult for Ford to marshal public support for his policies. With little experience in foreign affairs, Ford relied almost exclusively on Kissinger to pursue Nixon's aims of stability in the Middle East, rapprochement with China, and an easing of tensions with the Soviet Union.

Ford did make a change at the top of the National Security Council (NSC). Kissinger served as both national security adviser and secretary of state. During 1975, strong public and congressional disapproval developed over the accretion of so much power over foreign policy in the hands of one man. Watergate had discredited Nixon's system of a White House-centered system operating largely

independently of the various security agencies. Accordingly, as part of a cabinet shakeup on November 3, 1975, Ford replaced Kissinger as national security adviser with Lieutenant General Brent Scowcroft, who had been Kissinger's deputy at the NSC. This personnel shift produced little real change as Kissinger continued to dominate as the presidential advisor. Scowcroft acted in a low-key, low profile capacity while overseeing the flow of interdepartmental proposals and analyses of decisions.

Kissinger had two notable achievements under Ford. He managed to reduce Middle East tensions by persuading Egypt and Israel to rely on negotiations rather than force to settle future disagreements. He also presided over the Vladivostok treaty, signed by Ford and Soviet General Secretary Leonid Brezhnev in 1974. This pact, a continuation of the Strategic Arms Limitation Treaty (SALT) talks, was designed to serve as a basis for SALT II. It allowed each side to retain 2,400 strategic vehicles. This latter term was defined to include intercontinental ballistic missiles (ICBMs), submarine-launched ballistic missiles (SLBMs) such as the nuclear-powered Polaris, and, for the first time, intercontinental bombers. The land-based ICBMs are anti-missile missiles while the less-accurate SLBMs offer more security and are therefore regarded as a main deterrent force. Both the U.S. and U.S.S.R. were permitted to possess a limit of 1,320 multiple, independently targetable, reentry vehicles (MIRVs) on their ICBMs. It is essentially impossible to monitor the number of warheads within any missile without on-site inspections and, for this reason, MIRVs and other forms of multiple warhead systems had been omitted from consideration in the 1972 SALT agreement. Any anti-ballistic missile system is likely to be overwhelmed if the attack against it is from missiles with multiple warheads. On the other hand, a nation can withstand the loss of many retaliatory missiles and still have a formidable second-strike capability if the surviving ones are of the MIRV type.

Vladivostok raised concerns because neither the U.S. nor the Soviet Union possessed 2,400 strategic vehicles. The agreement seemed to many to be more of an arms expansion accord than an arms limitation one. The treaty also did nothing to address the existing inequity in large missiles, a category in which the Soviets were vastly superior.

While Ford faced attacks from Congress and the American public over Vladivostok, Cambodian Communists captured the American merchant ship *Mayaguez* in May, 1975. Ford sent the marines to rescue the crew, but initial public approval of this forceful act diminished when it was disclosed that the Cambodians had already agreed to release the Americans. Forty-one seamen died in the rescue. In that same month, South Vietnam fell to communist-controlled North Vietnam. Ford's tottering presidency received yet another blow when he stated, in televised debate with 1976 presidential opponent Jimmy Carter, that Eastern Europe was free of Soviet domination. Ford's defeat in the election meant that the Carter administration would negotiate the SALT II agreement.



## ■ FURTHER READING :

### BOOKS:

- Boll, Michael M. *National Security Planning Roosevelt through Reagan*. Lexington: University Press of Kentucky, 1988.
- Brodie, Bernard and Fawn M. Brodie. *From Crossbow to H-Bomb: The Evolution of the Weapons and Tactics of Warfare*. Bloomington: Indiana University Press, 1973.
- Carroll, Peter N. *It Seemed like Nothing Happened: America in the 1970s*. New Brunswick: Rutgers University Press, 1990.
- Crabb, Cecil V. and Kevin V. Mulcahy. *American National Security: A Presidential Perspective*. Pacific Grove, CA: Brooks/Cole, 1991.

### SEE ALSO

*Ballistic Missiles*  
*Cold War (1972–1989): The Collapse of the Soviet Union*  
*Middle East, Modern U.S. Security Policy and Interventions*  
*National Security Advisor, United States*  
*National Security Strategy, United States*  
*Nixon Administration (1969–1974), United States National Security Policy*  
*NSC (National Security Council)*  
*NSC (National Security Council), History*  
*Nuclear Weapons*

---

## Foreign Assets Control (OFAC), United States Office

---

The Office of Foreign Assets Control (OFAC) enforces economic and trade sanctions against foreign nations, drug traffickers, and terrorist organizations. The OFAC is part of the Department of the Treasury and acts under the authority of legislative controls and the wartime and national emergency power acts. Under these measures the OFAC has authority to trace and freeze foreign assets of those deemed to be a threat to national security.

The OFAC has its roots in the American Civil War. During this period, the Treasury Department sought and seized money and goods being traded or sold by the Confederacy under the Trading with the Enemy Act. During World War I, Congress updated the Treasury Department's authority under the revised Trading with the Enemy Act of 1917. In 1940 Congress sought to prevent the Nazis from using assets seized from the countries that Germany occupied by creating the Office of Foreign Funds Control (OFFC). After the United States entered World War II, the OFFC froze Axis assets and enforced the prohibition on trading with Axis nations.

President Truman established the current Office of Foreign Assets Control (OFAC) in 1950 as a reaction to Chinese involvement in the Korean War. The OFAC was charged with freezing and blocking all asset transfers by

China and North Korea. Although modified several times, American economic sanctions against North Korea have continued under The Foreign Assets Control Regulations since 1950.

Recently, the OFAC has been primarily concerned with tracing and freezing the assets of drug traffickers and terrorist organizations. The OFAC has played a key role in American efforts to cut funding to terrorist organizations since the September 11, 2001, terrorist attacks on the United States. Executive Order 13224 "Blocking Property and Prohibiting Transactions with Persons who Commit, Threaten to Commit, or Support Terrorism" granted the OFAC wide powers in administering and enforcing economic sanctions against suspected terrorist. This order also allowed the OFAC, in conjunction with the secretary of state and attorney general, to determine those responsible for funding terrorism and take appropriate action.

## ■ FURTHER READING :

### ELECTRONIC:

United States Department of Foreign Assets Control. <<http://www.ofac.gov/>>(05 January 2003).

### SEE ALSO

*Terrorist Organizations, Freezing of Assets*

---

## Foreign Intelligence Surveillance Act

---

The Foreign Intelligence Surveillance Act (FISA) was passed by the United States Congress in 1978 following an intensive investigation of the activities of U.S. intelligence and law enforcement agencies by the Church Committee.

The Church Committee (chaired by Sen. Frank Church) uncovered evidence of illegal wiretaps and illegal entry by the Federal Bureau of Investigation (FBI) as part of FBI efforts during the 1960s and early 1970s to conduct domestic surveillance on Vietnam War protesters and civil rights advocates.

FISA was also inspired by a ruling by the United States Supreme Court in 1972 (*United States v. U.S. District Court*), 407 U.S. 297, where the Supreme Court stated: "Given these potential distinctions between [Wiretap statute] criminal surveillances and those involving the domestic security, Congress may wish to consider protective standards for the latter which differ from those already prescribed for specified crimes [under the Wiretap statute]. Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens."

FISA established the United States Foreign Intelligence Surveillance Court and authorized the Court to conduct judicial oversight in matters of electronic surveillance related to intelligence and counterintelligence operation. The Court was composed of U.S. federal district court judges, appointed by the Chief Justice, who rotate membership on the court.

Because of the secret nature of the Court, and in order not to violate the Fourth Amendment of the Constitution (specifying the need for probable cause) warrants for surveillance were to be restricted to the gathering of information not intended to be used in criminal prosecution.

The Court reviews Justice Department applications for electronic surveillance. The Court meets two days each month and the proceedings are non-adversarial. Akin to grand jury procedures, the Court only considers arguments for surveillance brought by the Department of Justice Office of Intelligence Policy and Review.

FISA also broadly interpreted associations with “foreign power” so that individuals associated with foreign organizations designated as terrorist organizations by either the Court or Department of State are not entitled to the same Constitutional protections as individuals accuse of other crimes. FISA permits domestic surveillance if there is a judicial finding of probable cause that the individual or organization to be scrutinized acts for a foreign power. The acts constituting probable cause do not need to be criminal; they may, for example, fall into the realm civil economic activities. If the surveillance target is a U.S. citizen FISA requires that, in order to grant permission for surveillance based upon FISA, there must exist a probable cause to argue that the target’s acts involve espionage or other criminal conduct. FISA places a heavy reliance on “acts” so that U.S. citizens cannot be designated as agents of a foreign power “solely upon the basis of activities protected by the first amendment to the Constitution of the United States” (i.e. free speech rights).

Although initially limited to setting conditions for electronic surveillance, during the 1990s Congress expanded FISA to include provisions allowing physical searches.

It is estimated that FISA conditions applied to approximately 750 cases a year prior to the September 11, 2001, terrorist attacks on the U.S.

The Patriot Act, passed following the terrorist attacks on the United States on September 11, 2001, extended the government’s surveillance authority under FISA. New powers included roving wiretap authority (the surveillance of communications related to an individual or organization without regard to particular telephone line, computer station, or other mode of communication to be monitored. Other extensions included a more liberalized allowed use of pen register, trap and trace devices (removing the need to assert that the surveillance target is “an agent of a foreign power”). The lower Foreign Intelligence Surveillance Court specifically rejected Justice Department attempts at “information screening” and “minimization”

procedures are intended to allow the use of material gathered under Foreign Intelligence Surveillance Court authorization to criminal proceedings.

#### ■ FURTHER READING:

##### ELECTRONIC:

Electronic Privacy Information Center. Foreign Intelligence Surveillance Act (FISA) November 22, 2002. <<http://www.epic.org/privacy/terrorism/fisa/#Overview>> (April 15, 2003).

##### SEE ALSO

##### COINTELPRO

*Foreign Intelligence Surveillance Court of Review*

---

## Foreign Intelligence Surveillance Court of Review

---

The United States Foreign Intelligence Surveillance Court of Review is an appellate court for the review of matters related to espionage and counterintelligence.

Although the Court was established by the Foreign Intelligence Surveillance Act (FISA) passed by the United States Congress in 1978, the Court has had no record of meeting prior to its review of Justice Department electronic surveillance in September, 2002.

Following the terrorist attacks on the United States on September 11, 2001, the Justice Department’s use of domestic wiretaps increased and the department began to operate under broad new powers that Attorney General John Ashcroft asserted were granted to law enforcement agencies under the 2001 Patriot Act. A lower court, the Foreign Intelligence Surveillance Court—also authorized by FISA—ruled aspects of the Justice Department interpretation of those new powers to be unconstitutional. The Justice Department then appealed to the Foreign Intelligence Surveillance Court of Review, the first known appeal of a Foreign Intelligence Surveillance Court ruling.

The Court of Review operates as a three-judge panel composed of federal appellate judges—or retired appellate judges—appointed on a rotating basis by Chief Justice of the United States Supreme Court.

Court deliberations were conducted in secret and took place in an electronically secure room at the Justice Department. No public notice was given prior to the Court’s session and the Court issued no ruling or public statements following the session.

Congressional officials including Senate Intelligence and Judiciary Committee staff were denied requests to attend the appellate court’s initial hearing, according to

Justice Department officials, because the hearing contained detailed discussions of sources and methods used in intelligence gathering. Following congressional protests, the Court of Review, agreed to provide Senate Judiciary Committee members with an unclassified transcript of its proceedings and an unclassified copy of its rulings.

#### ■ FURTHER READING :

##### ELECTRONIC:

Electronic Privacy Information Center. November 22, 2002. <<http://www.epic.org/privacy/terrorism/fisa/#Overview>> (April 15, 2003).

##### SEE ALSO

*Church Committee  
COINTELPRO  
Patriot Act, United States  
Senate Select Committee on Intelligence, United States*

## Forensic Geology in Military or Intelligence Operations

■ WILLIAM C. HANEBERG

Forensic geology is strictly defined as the use of geologic principles and techniques to establish facts or provide evidence used in a court of law. A broader working definition includes the use of the same principles and techniques to establish facts or sequences of events regardless of whether they are used in court. Thus, the gathering and interpretation of geologic data for intelligence, espionage, and national security purposes can fall under the second definition of forensic geology. Forensic geology overlaps with the field of forensic soil science. In many cases, the work performed by practitioners in the two fields is very similar and the only distinction lies in the details of their academic training and professional experience. Also related is the field of forensic geophysics, in which geophysical instruments such as seismographs can be used as the basis for inferences about activities in remote or otherwise inaccessible areas.

**Origin of forensic geology.** The first written description of forensic geology is generally attributed to the fictional detective Sherlock Holmes, who was created by Arthur Conan Doyle (British, 1859–1930). In *A Study in Scarlet*, published in 1887, Holmes was endowed with the ability to easily distinguish soils of different types and infer from mud on their shoes and clothes the places to which people had traveled. He was also described by Dr. Watson, his

fictional colleague, as having a “practical, but limited” knowledge of geology.

The first real use of forensic geology to solve a crime does not appear to have occurred until 1904, when a German chemist named Georg Popp used geologic evidence to help identify a murder suspect from a handkerchief containing traces of snuff, coal dust, and the mineral hornblende. The prime suspect used snuff, and divided his labors between a coal gasification plant and a quarry in which the rocks were rich in the hornblende. (Coal gasification was then a common process in which coal was transformed into natural gas.) Soil in the suspect’s pant cuffs also was matched to soil at the crime scene and outside of the victim’s home. Taken together, the evidence convinced the suspect to confess. Four years later, Popp was able to show that one layer of soil on the shoes of a murder suspect matched the soil and distinctly green goose droppings around the suspect’s home. A second layer contained red sandstone fragments identical to those in the soil where the body was found. The third, and outermost, layer contained coal, brick, and cement dust identical to that found at the location where the murder weapon was found. The suspect claimed that he was walking in the fields near his home and therefore could not have committed the murder. Popp was able to show that, in addition to all of the geologic evidence that was preserved on the shoes, there was no sign of the distinctive milky white quartz particles that were characteristic of soil from those fields.

**Methods of forensic geology.** The methods used by forensic geologists are adaptations of the methods used by geologists engaged in academic research, mineral exploration, and other activities. For example, it is a fundamental principle of stratigraphy (the study of sequences of sedimentary rocks) that a layer of sedimentary rock is in most cases younger than the layers below it and older than the layers above it. This principle is known as the law of superposition. The implications for forensic geology are that a layer of mud deposited on shoes or an automobile is younger than the layers beneath it. Understanding the sequence of mud, sediment, or dirt layers can therefore allow forensic geologists to reconstruct a chain of events such as visits to several locations characterized by different soil or bedrock types.

Other techniques employed by forensic geologists are derived from the disciplines of petrography and petrology, which are concerned with the description and interpretation of rock types. Soils and rocks can be distinguished on the basis of their particle size distributions as well as the sphericity, angularity, and mineralogy of individual particles. Two samples of sand, for example, may be composed of grains that appear significantly different to an experienced geologist. Forensically important distinctions can sometimes be made with the unaided eye or a small magnifying lens. In other cases, binocular microscopes can be used to view grains using reflected light. A more elaborate method is the examination of thin sections

using transmitted polarized light. Thin sections are made by gluing a soil or rock to a glass slide and then grinding it to a standardized thickness of 30 microns. Most minerals are transparent in thin section (although a few metallic minerals remain opaque) and can be identified by their crystal shape and the degree to which they distort light passing through polarizing filters placed above and below the thin section. Fragments of macrofossils and intact microfossils, as well as pollen, in a soil or rock can likewise be identified by microscopy.

Particles smaller than sand grains can be difficult to identify using optical microscopes, but their shape and surface texture can be examined using instruments such as electron microscopes. Another class of instruments known as electron microprobes can perform non-destructive chemical analyses, including mapping variations in chemical composition across grains much less than a millimeter in diameter. Electron microprobe maps of oxygen content, for example, might be used to determine whether two metallic mineral grains have experienced similar degrees of oxidation.

The origin and history of a soil or rock particle is known as its provenance. Geologists in general and forensic geologists in particular can infer whether the source of sand grains is likely to have been an igneous or sedimentary rock, whether the grains were likely to have been transported by running water or exposed in an arid environment, and the climate in which a soil was formed. The presence of rare minerals or distinctive microfossils may allow them to further limit the possible sources to a small geographic area, perhaps a single watershed or rock body described in a published map or report. Thus, establishing the provenance of sand or mud recovered as forensic evidence can place a suspect at a crime scene or confirm an alibi.

**Forensic geology case histories.** There have been several publicly known cases in which forensic geology has played an important role in espionage, intelligence, security, and military operations.

During the second half of World War II, the Japanese military developed a plan to attack the United States with unmanned balloons carrying explosive and incendiary bombs. Using meteorological observations and calculations, they were able to design balloons that could be launched from Japanese beaches and carried by the jet stream to the western United States. The balloons were designed to be self-regulating, releasing sandbags in order to gain elevation during cold nights and releasing hydrogen to lose elevation during warm days. It is believed that 9000 balloons were launched, of which an estimated 1000 reached North America. Two balloons drifted as far east as Michigan. Although they ignited a few small fires and killed only six people (five children and a minister's wife who came across an unexploded bomb while on a fishing trip in Oregon), their origin was of concern. It was not known whether the balloons were

being launched from Japanese submarines, by shore parties that had landed on American beaches, from German prisoner of war camps, or from the internment camps to which many Japanese-American citizens had been forcibly relocated. Geologists in the military geology unit of the U.S. Geological Survey were asked to determine the launching point of the balloons from the provenance of sand that had been used for ballast and which had been recovered from many balloon crash sites. Because sand has a low economic value and is expensive to transport, it was likely that the source of the sand was at or near the launching areas. The geologists first eliminated North American sources for the sand, which contained an unusual combination of minerals, fossil and recent diatoms (single celled algae that secrete siliceous cell walls), foraminifera (single celled organisms with calcareous shells), mollusk shell fragments, and no coral. The absence of coral was important because coral grows only in warm water, meaning that the sand most likely came from a northern area. By comparing the sand to geologic maps and reports that had been published before the war, one as early as 1889, the geologists suggested two possible launching sites along the northern coast of Japan. In reality, balloons were being launched from three sites. One of them was a site identified by the geologists and the other two, separated by approximately 15 km, were close to the second site identified by the geologists.

Forensic geology has also been used to investigate politically motivated murders and terrorist attacks. Grains of sand and microfossils found on the body of Italian Prime Minister Aldo Moro, who was kidnapped and murdered by Red Brigade terrorists in 1978, led investigators to conclude that he had been held at least part of the time along an 11 km long stretch of beach north of Rome. The total mass of sand collected from Moro's clothing and the car in which his body was discovered was approximately 1 gram. The presence of bitumen (a tar-like substance in this case derived from oil spills dispersed by waves) and resins used in boat building further supported the beach hypothesis. Because of the high profile and political sensitivity of the case, collection of sand samples for comparison with the grains found on Moro's body occurred in secret. The geologist working on the case was accompanied by his wife, who posed as a tourist picking plants and observing the scenery while her husband surreptitiously collected sand samples.

The Federal Bureau of Investigation (FBI) relied heavily on geologic evidence to learn how the Mexico Federal Judicial Police (MFJP) attempted to cover up the murder of Drug Enforcement Agency (DEA) agent Enrique Salazar and pilot Alfredo Avelar, who assisted Salazar on clandestine missions for the United States government. Salazar had been kidnapped at gunpoint from the streets of Guadalajara, Mexico and his body was discovered, along with that of Avelar, after a shootout between the MFJP and family engaged in the drug trade. The entire family was killed in the shootout, and the implication was that Salazar had been kidnapped and killed by the family. Traces of soil

on the bodies of Salazar and Avelar, however, did not match the soil at the ranch where the shootout occurred and caused suspicion to be cast on the explanation offered by the Mexican government. Detailed studies by an FBI geologist posing as a DEA agent (FBI agents were not allowed to work in Mexico, but DEA agents were) revealed an extremely uncommon assemblage of mineral grains and shards of pink volcanic glass. This geologic evidence led the investigators to a state park in mountainous terrain where, based on detailed examination of individual soil particles, the site at which Salazar and Avelar had originally been buried was discovered. Other forensic evidence showed that the MFJP had been involved in the kidnapping, torture, and burial of Salazar and Avelar.

Geologic interpretation of photographs and videotapes can also shed light on the location in which a photograph or a recording was made. A notable example of this kind of forensic geology occurred shortly after the September 11, 2001 terrorist attacks on the World Trade Center in New York City and the Pentagon in Washington, D.C. American geologists who had worked in Afghanistan were able to identify rocks in the background of a videotaped message from the terrorist leader Osama bin Laden, and therefore the region of the country in which the message was taped. The use of geologic knowledge to infer location was widely publicized, however, and subsequent messages were recorded against a cloth background in order to prevent the location of the taping from being discerned.

Knowledge of the principles of forensic geology can be used to obscure evidence or mislead investigators. Double agent Kim Philby (British, 1912–1988), who spied for the Soviet Union while at the same time working in the British intelligence service during the Cold War years, once used a small trowel to bury a camera in a wooded area near the Potomac River in Virginia. He then returned to his home and used the trowel to dig in his garden in order to obscure any soil particles that might be used to identify the location of the camera. This incident would never have been known if Philby had not described it in his autobiography. Terrorists arrested in conjunction with the Aldo Moro case insisted that forensic evidence had been planted in order to steer authorities away from the true location of their activities, which might have led to the arrest of additional suspects. It appears, though, that the forensic evidence was authentic and reliable.

**Forensic seismology.** The use of geophysical methods, especially those derived from seismological studies of the Earth, can also provide information about remote events. Analysis of seismograms produced by the explosion of the Russian submarine Kursk in 2000, for example, have shown that a small initial explosion was followed by a much larger explosion that produced vibrations equivalent to those from a magnitude 4.1 earthquake. This information was used to infer that the size of the explosion was equivalent to that which would have been produced by 4000 to 6000 kilograms of TNT. Seismologists were also

able to analyze information about the oscillations of a bubble of hot gas that rose through the sea after the explosion, and infer that the main explosion took place at a depth of approximately 100 meters. Bathymetric data suggest that the seafloor is about 100 meters deep at the explosion site, so it is likely that the second explosion occurred when the sinking submarine struck the seafloor.

Seismological data have also been used to help infer the details of 1995 bombing of the Murrah Federal Building in Oklahoma City, the 2001 World Trade Center attack, and the 2001 Pentagon attack. Analysis of seismograms associated with the collapse of the World Trade Center towers, for example, suggests that the actual structural collapse occurred over a period of about three seconds. The same principles can be used to obtain evidence of clandestine conventional or nuclear explosions, and in particular to verify that nuclear test ban treaties are not being violated.

Seismological data may provide information about the February 2003 disintegration of the space shuttle Columbia. The sonic boom produced as a shuttle descends is normally recorded on seismographs, but the seismogram produced by the final Columbia reentry does not contain evidence of a sonic boom. Although the reasons for this were unclear at the time this article was written, the seismic data provided enough information to allow the location of the disintegration to be calculated and compared against other observations.

## ■ FURTHER READING:

### BOOKS:

- Mikesh, Robert C. *Japan's World War II Balloon Bomb Attacks on North America*. Washington, D.C.: Farrar, Smithsonian Institution Press. 1990.
- Murray, R. C. and J. C. Tedrow. *Forensic Geology*. Englewood Cliffs, New Jersey: Prentice Hall, 1998.

### PERIODICALS:

- Buck, S. "Searching for Graves Using Geophysical Technology: Field Tests with Ground Penetrating Radar, Magnetometry, and Electrical Resistivity." *Journal of Forensic Sciences*, vol. 48, no. 1 (2003): 5–11.
- Holzer, T. L., J. B. Fletcher, G. S. Fuis, T. Ryberg, T. M. Brocher, and C. M. Dietel. "Seismograms Offer Insight into Oklahoma City Bombing." *Eos, Transactions American Geophysical Union*, vol. 77, no. 41 (October 8, 1996): 393, 396–397.
- Koper, K. D., T. C. Wallace, S. R. Taylor, and H. E. Hartse. "Forensic Seismology and the Sinking of the Kursk." *Eos, Transactions, American Geophysical Union*, vol. 82, no. 4 (2001): 37.
- Lombardi, Gianni. "The Contribution of Forensic Geology and Other Trace Evidence Analysis to the Investigation of the Killing of Italian Prime Minister Aldo Moro." *Journal of Forensic Sciences*, v. 44, no. 3 (1999): 634–642.
- McPhee, John. "Annals of Crime—The Gravel Page." *The New Yorker*. (January 29, 1996): 44–69.

**ELECTRONIC:**

American Society of Forensic Geologists. "American Society of Forensic Geologists." 2002. <<http://www.forensicgeology.org/>>(13 March 2003).

Levine, Alissa. "Secrets Hidden in Soil." September 5, 2001. <<http://tpwww.gsfc.nasa.gov/globe/forengeo/secret.htm>>(13 March 2003).

Murray, Raymond. "Devil in the Details, the Science of Forensic Geology." January 29, 2003. <<http://www.forensicgeology.net/science.htm>>(13 March 2003).

Pinsker, Lisa M. "Geology Adventures in Afghanistan." Geotimes Web Feature. February 2002. <[http://www.agiweb.org/geotimes/feb02/Feature\\_Shroderside.html](http://www.agiweb.org/geotimes/feb02/Feature_Shroderside.html)>(13 March 2003).

**SEE ALSO**

*Geologic and Topographical Influences on Military and Intelligence Operations*

*Geospatial Imagery*

*GPS*

*Mapping Technology*

*Seismograph*

*Seismology for Monitoring Explosions*

*Weapons of Mass Destruction, Detection*

---

## Forensic Science

---

■ AGNIESZKA LICHANSKA

Forensic science is a multidisciplinary subject used for examining crime scenes and gathering evidence to be used in prosecution of offenders in a court of law. Forensic science techniques are also used to examine compliance with international agreements regarding weapons of mass destruction.

The main areas used in forensic science are biology, chemistry, and medicine, although the science also includes the use of physics, computer science, geology, and psychology. Forensic scientists examine objects, substances (including blood or drug samples), chemicals (paints, explosives, toxins), tissue traces (hair, skin), or impressions (fingerprints or tidemarks) left at the crime scene. The majority of forensic scientists specialize in one area of science.

### Evidence and Trace Examination

The analysis of the scene of crime or accident involves obtaining a permanent record of the scene (forensic photography) and collection of evidence for further examination and comparison. Collected samples include biological (tissue samples such as skin, blood, semen, or hair),

physical (fingerprints, shells, fragments of instruments or equipment, fibers, recorded voice messages, or computer discs) and chemical (samples of paint, cosmetics, solvents, or soil).

Most commonly, the evidence collected at the scene is subsequently processed in a forensic laboratory by scientists specializing in a particular area. Scientists identify, for example, fingerprints, chemical residues, fibers, hair, or DNA left behind. However, miniaturization of equipment and the ability to perform most forensic analysis at the scene of crime results in more specialists being present in the field. Presence of more people at the scene of crime introduces a greater likelihood of introduction of contamination into the evidence. Moreover, multi-handling of a piece of evidence (for example a murder weapon being analyzed by many specialists) is also likely to introduce traces of tissue or DNA not originating from the scene of a crime. All this results in strict quality controls imposed on collection, handling, and analysis of evidence to ensure lack of contamination. For example, in DNA analysis it is essential that samples are stored at the correct temperature and that there is no contamination from a person handling a sample by wearing clean gloves and performing analysis in a clean laboratory.

Ability to properly collect and process forensic samples can affect the ability of the prosecution to prove their case during a trial. The presence of chemical traces or DNA on a piece of debris is also crucial in establishing the chain of events leading to a crime or accident.

A growing area of forensic analysis is monitoring non-proliferation of weapons of mass destruction, analysis of possible terrorist attacks or breaches of security. The nature of samples analyzed is wide, but slightly different to a criminal investigation. In addition to the already described samples, forensic scientists who gather evidence of mass destruction collect swabs from objects, water, and plant material to test for the presence of radioactive isotopes, toxins, or poisons, as well as chemicals that can be used in production of chemical weapons. The main difference from the more common forensic investigation is the amount of chemicals present in a sample. Samples taken from the scene of suspected chemical or biological weapons often contain minute amounts of chemicals and require very sensitive and accurate instruments for analysis.

**Biological traces.** Biological traces are collected not only from the scene of crime and a deceased person, but also from surviving victims and suspects. Most common samples obtained are blood, hair, and semen. DNA can be extracted from any of these samples and used for comparative analysis.

DNA is the main method of identifying people. Victims of crashes or fires are often unrecognizable, but adequate DNA can be isolated and a person can be positively identified if a sample of their DNA or their family's



A member of the International Commission on Missing Persons in Bosnia, inspects human remains found by forensics experts in a mass grave at the village of Kamenica, an area of Serbian-controlled Bosnia, in 2002. AP/WIDE WORLD PHOTOS.

DNA is taken for comparison. Such methods are being used in the identification of the remains in Yugoslav war victims, the World Trade Center terrorist attack victims, and the 2002 Bali bombing victims.

Biological traces, investigated by forensic scientists come from bloodstains, saliva samples (from cigarette butts or chewing gum) and tissue samples, such as skin, nails, or hair. Samples are processed to isolate the DNA and establish the origin of the samples. Samples must first be identified as human, animal, or plant before further investigation proceeds. For some applications, such as customs and quarantine, traces of animal and plant tissue have to be identified to the level of the species, as transport of some species is prohibited. A presence of a particular species can also prove that a suspect or victim visited a particular area. In cases of national security, samples are tested for the presence of pathogens and toxins, and the latter are also analyzed chemically.

**Chemical traces.** Forensic chemistry performs qualitative and quantitative analysis of chemicals found on people, various objects, or in solutions. The chemical analysis is the most varied from all the forensic disciplines. Chemists analyze drugs as well as paints, remnants of explosives,

fire debris, gun shot residues, fibers, and soil samples. They can also test for a presence of radioactive substances (nuclear weapons), toxic chemicals (chemical weapons) and biological toxins (biological weapons). Forensic chemists can also be called on in a case of environmental pollution to test the compounds and trace their origin. The samples are obtained from a variety of objects and often contain only minute amounts of chemicals.

The identification of fire accelerants such as kerosene or gasoline is of great importance for determining the cause of a fire. Debris collected from a fire must be packed in tight, secure containers, as the compounds to be analyzed are often volatile. An improper transport of such debris would result in no detection of important traces. One of the methods used for this analysis involves the use of charcoal strips. The chemicals from the debris are absorbed onto the strip and subsequently dissolved in a solvent before analysis. This analysis allows scientists to determine the hydrocarbon content of the samples and identify the type of fire accelerator used.

**Physical evidence.** Physical evidence usually involves objects found at the scene of a crime. Physical evidence may include all sorts of prints such as fingerprints, footprints,

handprints, tidemarks, cut marks, tool marks, etc. Analysis of some physical evidence is conducted by making impressions in plaster, taking images of marks, or lifting the fingerprints from objects encountered. These serve later as a comparison to identify, for example, a vehicle that was parked at the scene, a person that was present, a type of manufacturing method used to create a tool, or a method used to break in a building or harm a victim.

An examination of documents found at the scene or related to the crime is often an integral part of forensic analysis. Such examination is often able to establish not only the author, but more importantly identify any alterations that have taken place. Specialists are also able to recover text from documents damaged by accident or on purpose.

**Identification.** The identification of people can be performed by fingerprint analysis or DNA analysis. When none of these methods can be used, the facial reconstruction can be used instead to generate a person's image. TV and newspapers then circulate the image for identification.

## Other Forensic Scientists

Pathologists and forensic anthropologists play a very important part in forensic examination. They are able to determine the cause of death by examining marks on the bone(s), skin (gunshot wounds), and other body surfaces for external trauma. They can also determine a cause of death by toxicological analysis of blood and tissues.

A number of analytical methods are used by forensic laboratories to analyze evidence from a crime scene. Methods vary, depending on the type of evidence analyzed and information that needs to be extracted from the traces found. If a type of evidence is encountered for the first time, a new method is developed.

Biological samples are most commonly analyzed by polymerase chain reaction (PCR). The results of PCR are then visualized by gel electrophoresis. Forensic scientists tracing the source of a biological attack could use the new hybridization or PCR-based methods of DNA analysis. Biological and chemical analysis of samples can identify toxins found.

Imaging used by forensic scientists can be as simple as a light microscope, or can involve an electron microscope, absorption in ultraviolet to visible range, color analysis or fluorescence analysis. Image analysis is used not only in cases of biological samples, but also for analysis of paints, fibers, hair, gunshot residue, or other chemicals. Image analysis is often essential for an interpretation of physical evidence. Specialists often enhance photographs to visualize small details essential in forensic analysis. Image analysis is also used to identify details from surveillance cameras.

The examination of chemical traces often requires very sensitive chromatographic techniques or mass spectrometric analysis. Four major types of chromatographic methods used are: thin layer chromatography (TLC) to separate inks and other chemicals, atomic absorption chromatography for analysis of heavy metals, gas chromatography (GC), and liquid chromatography (HPLC). GC is most widely used in identification of explosives, accelerators, propellants, and drugs or chemicals involved in chemical weapon production, while liquid chromatography (HPLC) is used for detection of minute amounts of compounds in complex mixtures. These methods rely on separation of the molecules based on their ability to travel in a solvent (TLC) or to adhere to adsorbent filling the chromatography column. The least strongly absorbed compounds are eluted first and the most tightly bound last. By collecting all of the fractions and comparing the observed pattern to standards, scientists are able to identify the composition of even the most complex mixtures.

New laboratory instruments are able to identify nearly every element present in a sample. Because the composition of alloys used in production of steel instruments, wires or bullet casings is different between various producers, it is possible to identify a source of the product.

In some cases chromatography alone is not an adequate method for identification. It is then combined with another method to separate the compounds even further and results in greater sensitivity. One such method is mass spectrometry (MS). A mass spectrometer uses high voltage to produce charged ions. Gaseous ions or isotopes are then separated in a magnetic field according to their masses. A combined GC-MS instrument has a very high sensitivity and can analyze samples present at concentrations of one part-per-billion.

As some samples are difficult to analyze with MS alone, a laser vaporization method (imaging laser-ablation mass spectroscopy) was developed to produce small amounts of chemicals from solid materials (fabrics, hair, fibers, soil, glass) for MS analysis. Such analysis can examine hair samples for presence of drugs or chemicals. Due to its high sensitivity, the method is of particular use in monitoring areas and people suspected of production of chemical, biological or nuclear weapons, or narcotics producers.

While charcoal sticks are still in use for fire investigations, a new technology of solid-phase microextraction (SPME) was developed to collect even more chemicals and does not require any solvent for further analysis. The method relies on the use of sticks similar to charcoal, but coated with various polymers for collecting different chemicals (chemical warfare agents, explosives, or drugs). Collected samples are analyzed immediately in the field in by GC.

A number of instruments used are smaller than ever before, allowing them to be used directly in the field with rapid results. For example, a combined GC-MS analysis



device can analyze a sample within 15 minutes directly in the field. The standard laboratory instrument is large with a weight over 100 kilograms, while the portable version is only 28 kilograms. A number of government agencies (for example the FBI) are now armed with the portable instruments and can perform rapid forensic analysis in the field in a time shorter than it would take to transport samples to a forensic laboratory. United States troops are equipped with similar instruments on board some tanks and trucks, in order to quickly determine the presence of chemical or biological weapons on the battlefield

**Applications of forensic science.** The main use of forensic science is for purposes of law enforcement to investigate crimes such as murder, theft, or fraud. Forensic scientists are also involved in investigating accidents such as train or plane crashes to establish if they were accidental or a result of foul play. The techniques developed by forensic science are also used by the army to analyze the possibility of the presence of chemical weapons, high explosives or to test for propellant stabilizers. Gasoline products often evaporate rapidly and their presence cannot be confirmed, but residues of chemicals, such as propellant stabilizers, are present for much longer indicating that an engine or missile was used.

#### ■ FURTHER READING:

- Houde, John. *Crime Lab: A guide for Nonscientists*. Rolling Bay: Calico Press, 1998.
- Kelly, John F., and Phillip K, Wearne. *Tainting Evidence: Inside the Scandals at the FBI Crime Lab*. New York: Free Press, 1998.
- Saferstein, Richard. *Criminalistics: An Introduction to Forensic Science*. New York: Prentice-Hall, 2000.

#### ELECTRONIC:

- American Academy of Forensic Science <<http://www.aafs.org>> (7 February 2003).
- Consulting and Duction in Forensic Science. "Forensic Science Timeline." Norah Rudin. <<http://www.forensicdna.com/Timeline.htm>>(7 February 2003).
- Forensic Science Center, University of California Lawrence Livermore National Laboratory, 7000 East Ave., Livermore, CA 94550–9234. (925) 423–1189. <<http://www.llnl.gov/IPandC/op96/10/10h-for.html>> (7 February 2003).
- Forensic Science Web Pages. 7 February 1997. <<http://home.earthlink.net/~thekeither/Forensic/forsone.htm>>(7 February 2003).
- National Center for Forensic Science, University of Central Florida 12354 Research Parkway Orlando, FL 32826. (407) 823–6469. <<http://ncfs.ucf.edu/navbar.html>> (7 February 2003).

#### SEE ALSO

*Chemistry: Applications in Espionage, Intelligence, and Security Issues*

*DNA Recognition Instruments*  
*Document Forgery*  
*Gas Chromatograph-Mass Spectrometer*  
*Isotopic analysis*  
*Polymerase Chain Reaction (PCR)*  
*Thin Layer Chromatography*

## Forensic Voice and Tape Analysis

Methods of forensic voice and tape analysis first entered the limelight during the Watergate scandal in the early 1970s, and the basic methodology—if not the tools and precision with which the techniques are practiced—has changed little since. Much of this field is concerned with identification or elimination using voice-stress analysis, but controversy over techniques and their admissibility as evidence remains. This disagreement, even among specialists, came to the forefront as forensic scientists on both sides of the Atlantic studied tapes allegedly released by terrorist mastermind Osama bin Laden in the fall of 2002.

**Early history.** Spectrographic analysis and related techniques make it possible to match a suspect to an incriminating sample of his or her speech—a threatening phone call, for instance, or a taped admission of guilt. Voice and tape analysis can also be used to clear a suspect. In this field, a scientifically verified match between a suspect (or another individual) and a voice sample is known as an identification, while scientific proof, by means of voice analysis, that a suspect and a voice sample do not match is called an elimination.

The U.S. Federal Bureau of Investigation (FBI) used spectrographic or voice identification analysis as early as the 1950s, but the technique did not gain scientific acceptance until a 1962 study by Lawrence Kersta, a researcher working with a 1940s-model Bell Laboratory sound spectrograph. Kersta maintained that “voiceprints,” a term he coined, provide a unique means of identifying individuals. He went on to establish a professional association, the International Association of Voice Identification, which in 1980, became part of the more general International Association for Identification.

**The 1970s.** The word “voiceprint” would later be discarded, due to the false association with fingerprinting, which is a much more exact science. Nevertheless, spectrographic techniques continued to gain respect in forensic and law enforcement circles, thanks in part to a 1972 study at

Michigan State University. The study found an error rate of two percent for false identification (instances in which the examiner chose the wrong match, or found a match when none existed), and five percent for false elimination, in which the examiner failed to recognize that a match existed. In the years immediately following this study, spectrographic techniques came to widespread public attention during the examination of tapes made by President Richard M. Nixon in the White House.

In 1979, a National Research Council committee presented the FBI with the results of a study on spectrographic voice identification under forensic conditions, involving some 2,000 forensic comparisons made by FBI personnel. The researchers' findings confirmed the impression that, while it was not an exact science, voice analysis could be useful. According to the study, error rates varied as a function of the properties of the voice studied, the conditions and techniques used, and the examiners' skills and knowledge.

**Voice analysis today.** The period since the 1970s has seen considerable evolution in spectrographic analysis and the related methods and tools, which include evidence handling, critical listening, magnetic development, waveform analysis, spectrum analysis, tape enhancement, and speed correction. The core methodology, however, remains the same; from machine readings of stress and other patterns in a subject's voice, a graphic representation is made so as to illustrate patterns of frequency, intensity, pitch, and inflection. Analysts use a two-step process, first the aural or listening stage, then the visual stage, which involves looking over the spectrograms or readouts.

Spectrographic analysis remains controversial. It is permissible as evidence in 35 of 50 states, and has a status—both in the eyes of the law and of professionals—akin to that of polygraphy or lie detection; although not perfectly reliable, it can be a helpful tool for screening suspects. Controversy over spectrographic analysis came to the forefront in November, 2002, when the Arabic news station al Jazeera released a recording of an alleged telephone call from bin Laden.

Analysts working for the U.S. Central Intelligence and National Security agencies studied, and verified the authenticity of, the tape, in which the voice spoke of recent terrorist actions and promised to unleash more attacks. At the Institute for Perceptual Artificial Intelligence in Switzerland, however, researchers were not as certain. Using biometric software, they judged it a 55%–60% likelihood that the tape was not genuine.

#### ■ FURTHER READING:

##### BOOKS:

Gardner, Robert. *Crime Lab 101: Experimenting with Crime Detection*. New York: Walker, 1992.

Ross, David F., and J. Don Read. *Adult Eyewitness Testimony: Current Trends and Developments*. New York: Press Syndicate of the University of Cambridge, 1994.

Saferstein, Richard. *Criminalistics: An Introduction to Forensic Science*. NJ: Prentice Hall, 1998.

##### PERIODICALS:

Romanko, J. R. "Truth Extraction." *New York Times Magazine*. (November 19, 2000): 54.

##### ELECTRONIC:

Sachs, Jessica Snyder. Graphing the Voice of Terror. *Popular Science*. <<http://www.popsci.com/popsci/science/article/0,12543,426271,00.html>> (April 13, 2003).

##### SEE ALSO

*Forensic Science*  
*Polygraphs*  
*Voice Alteration, Electronic*

---

## France, Counter-Terrorism Policy

---

Counter-terrorism is the use of military, law enforcement, intelligence, and other resources to identify, circumvent, and neutralize terrorist groups within a country. Like all western European nations, France has been forced by events since the 1960s to develop a response to terrorism. The most attention-getting aspect of French counter-terrorism is GIGN, the Group d'Intervention de la Gendarmerie Nationale (National Police Intervention Group), but this small, elite counter-terrorism action team is only a small component of counter-terrorism activities and policy in France.

Overseeing and coordinating antiterrorist activity in France is the Interministerial Liaison Committee against Terrorism, or Comité Interministériel de Lutte Anti-Terroriste. The committee, which includes the prime minister and the ministers of the Interior, Defense, Justice, and Foreign Affairs, develops and directs counter-terrorism policy. Below the committee in rank is the Anti-Terrorism Coordination Unit (Unité de Coordination de la Lutte Anti-Terroriste), which includes agencies from the Interior and Defense ministries, and which coordinates operations.

Unlike in the United States, where the Department of the Interior manages natural resources, France's Ministry of the Interior (Ministère de L'Intérieur) is a security and law-enforcement department. The ministry, which oversees the Anti-Terrorism Coordination Unit, includes the National

Police, the Central Headquarters for Surveillance of the Territory, and the General Intelligence Central Service. All of these services are responsible for law enforcement and/or monitoring of suspicious activities in French territories.

**Enforcement agencies.** The National Police, or Direction Générale de la Police Nationale, is the principal civilian national police force in large urban areas. Within the National Police are specialized groups with functions such as border security and the protection of dignitaries. In addition to the National Police, which falls under the Ministry of the Interior, there is the National Gendarmerie, or Direction Générale de Gendarmerie Nationale, directed by the Ministry of Defense. The National Gendarmerie oversees law enforcement in small towns and rural areas.

Also under the Ministry of Defense is GIGN, which, like its German counterpart, GSG-9, was formed in the aftermath of the terrorist incident at the 1972 Munich Olympics. GIGN, though highly effective in special circumstances, is a small force, consisting of fewer than a hundred full-time personnel at the end of the twentieth century. Its activities are, therefore, rather limited compared to those of larger police forces.

**Intelligence agencies.** The Central Headquarters for Surveillance of the Territory (Direction de la Surveillance du Territoire), an arm of the National Police, gathers intelligence regarding potential threats from external organizations. Overseeing potential threats by internal organizations is the General Intelligence Central Service (Direction Centrale des Renseignements Généraux).

Outside of France, intelligence gathering is the job of the General Headquarters for Security Overseas (Direction Générale de la Sécurité Extérieure), which is under the Ministry of Defense. The Central Headquarters Military Intelligence (Direction Renseignements Militaire), also under the Ministry of Defense, gathers and interprets military intelligence.

#### ■ FURTHER READING :

##### BOOKS:

Bourret, Jean Claude. *GIGN, Vingt Ans d'Actions: 1974–1994*. Paris: M. Lafon, 1995.

Linde, Erik J. G. van de. *Quick Scan of Post 9/11 National Counter-terrorism Policymaking and Implementation in Selected European Countries: Research Project for the Netherlands Ministry of Justice*. Santa Monica, CA: RAND Europe, 2002.

##### PERIODICALS:

Hoffman, Bruce. "Is Europe Soft on Terrorism?" *Foreign Policy* no. 115 (summer 1999): 62–76.

#### SEE ALSO

*European Union*  
*France, Intelligence and Security*  
*Germany, Counter-Terrorism Policy*

## France, Intelligence and Security

■ ADRIENNE WILMOTH LERNER

Although France has employed espionage agents since the Middle Ages, the modern intelligence community emerged in the nineteenth century. As France expanded its boundaries during the Napoleonic era and Age of Empire, military intelligence was equally crucial to the success of battlefield operations and the security of territorial government outposts. At the outbreak of World War I in 1914, France maintained one of the most skilled and well-organized intelligence forces in the world. Modern domestic intelligence can trace its roots to the revolution, but it was most acutely influenced by the formation and operation of underground Resistance groups during the World War II Nazi Occupation. Vichy France and French officials who collaborated with the Nazis left a legacy of mistrust of and within the government in the years following the war. These tensions were heightened by the onset of the Cold War. When France began the process of recreating its intelligence systems, it placed special emphasis on domestic and political intelligence.

The French intelligence community is divided between military and civilian agencies, all of which report to the executive branch. The civilian intelligence system emphasizes counter-intelligence and domestic security. This requires not only the substantial national intelligence and security structure, but also the assistance and continued cooperation of provincial security and law enforcement agencies. External intelligence is almost exclusively dominated by the military. This separation of powers gives military and civilian intelligence organizations their own *de facto* jurisdictions in the intelligence community.

French military intelligence is administered by the individual military branches (Army, Navy, and Air Force) and the Ministry of Defense. The National Defense General Secretariat (SDGN) coordinates intelligence and security operations within the various intelligence community agencies. Military intelligence, as well as strategic information and counter-espionage operations, is directed by the General Directorate for External Security (DSGE). The agency employs analysts as well as active field operatives, and is the primary foreign intelligence agency. The Directorate of Military intelligence performs many of the same

plenary and investigative functions as the DSGE, but does not have an active field operations branch.

Military counterintelligence is charged to two agencies, the Directorate for the Defense Protection and Security (DPSD) and the Intelligence and Electronic Warfare Brigade (BRGE). The DPSD is the primary military counterintelligence agency, planning and coordinating most military security operations. The agency also conducts political surveillance of the armed forces and national military police, the Gendarmerie. The BRGE works closely with the DPSD, and is charged with monitoring sensitive communications and securing military computer information systems.

Civilian intelligence agencies operate under the directorship of the Ministry of the Interior. The General Information Service (RG) is the main domestic intelligence agency in the French government. The director of the RG reports to the minister of the Interior and briefs the president on domestic national security issues. Charged with the protection of internal security and domestic counterintelligence, the RG works in close conjunction with provincial governments and prefectures of the national police to protect national interests within France.

In French territories, the Directorate of Territorial Security (DST) performs the functions of the RG. The DST works closely with military intelligence units to protect French interests throughout the world. In twenty-first century anti-terrorist intelligence operations, the DST and RG have infiltrated and arrested several persons with alleged connections terrorist groups smuggling money and weapons via French territories. The DST also focuses on protecting French scientific, research, and economic interests abroad.

In recent years, French intelligence and security forces have grappled with increasing terrorist threats, mostly from members of North African, Islamist militant groups. After the September 11, 2001, attacks on the United States, France joined an international intelligence coalition to find and dismantle terrorist organizations and their operative cells.

## ■ FURTHER READING:

### BOOKS:

Porch, Douglas. *The French Secret Services: From the Dreyfus Affair to the Gulf War*. New York: Farrar, Straus & Giroux, 1995.

### PERIODICALS:

Porch, Douglas. "French Intelligence Culture: A Historical and Political Perspective." *Intelligence and National Security* 10, no. 3 (Jul. 1995): 486–511.

### SEE ALSO

*European Union*

# French Underground during World War II, Communication and Codes

■ ADRIENNE WILMOTH LERNER

By 1940, Nazi Germany had invaded several Eastern European nations and turned its attention to gaining control of Western Europe. With strategic planning reminiscent of World War I, the Nazis planned to forcefully invade France, Belgium, and Holland. However, when Marshal Henri-Philippe Petain rose to power in France, he negotiated an armistice with the Germans. On June 22, France was divided into two parts: the northern three-fifths and the Atlantic coast to be directly controlled by Nazi Germany, and the remaining parts of the south to be ruled by a French puppet government. The southern region was known as Vichy. The armistice also disbanded the French army, sending many French soldiers who could escape into exile in England. The settlement angered many French citizens, many of whom wished to continue the war against Germany.

As soon the occupation began, partisan groups arose to sabotage the Nazi government. These groups called themselves by many names (maquis, partisans, resistance, and freedom fighters) and the individual groups remained separate entities until the Allied invasion of France in 1944. These underground bands of French and foreign men and women who fought against the German occupation government became known collectively as the French Resistance.

The German secret police, the Gestapo, and intelligence agency, Abwehr, were powerful opponents to the resistance. In the early war period, German agents easily infiltrated resistance groups. In response, resistance groups developed codes, complex communications networks, and security structures to protect members and information.

Many of the earliest resistance groups were formed by political parties that the Nazi government had earlier banned. Communists and Socialists were persecuted under the Nazi regime. Partisan groups with political ties, such as the Socialist *Comité d'Action Socialiste* and the Communist *Front National* used their extensive media and member network to produce and distribute anti-Nazi propaganda. As resistance groups began to arm themselves and carry out acts of sabotage, the papers published coded messages that communicated instructions to members. During the course of the war, underground newspapers supplied information to over a million readers.

The resistance relied on coded messages to communicate with members and plan operations. Members were called by code names, and operational units had their own cryptonym or symbols. Underground newspaper published coded articles and drawings. Poetry was even used

as a means of sending coded messages or identifying oneself as a member of a resistance group to other members.

The most famous, and perhaps ingenious security device of resistance groups was the use of a pyramid command structure. The pyramid structure ensured that no member of a partisan group even interacted or conducted operations with more than two other members of the organization. No records of membership were kept, and messages were sent only by word-of-mouth. Each resistance member knew one commanding member and one other partner member. Members kept strict confidentiality, and rarely met in groups larger than their operational units. This structure insured that enemy infiltrators and captured partisans could positively identify no more than two resistance operatives, leaving the rest of the organization unscathed. The strategy worked with some success, until Gestapo agents began to infiltrate the command echelons of various partisan groups.

The pyramid structure also added an operational advantage as well as security. Ambushes and assassinations of German officers were carried out by a group of three men. One man served as a decoy, the other carried the weapon and shot the victim at close range, while the third member took the weapon after the shooting and walked away from the scene. Often the actual assailants would remain at or near the scene until authorities arrived. As they possessed no weapons, they were cleared of suspicion. Because resistance members in most urban areas did not keep their own weapons as a security measure, weapons used in attacks were returned to their stockpile via courier, often a child, who would seldom arouse the suspicion of Gestapo agents.

French Resistance groups also developed an “underground railroad” system to smuggle downed Allied airmen back to Britain or the front lines. Using standardized coded messages, Allied servicemen were shuttled to various safe houses on route to their destination. Toward the end of the war, these same networks were used by Allied forces to send messages to various resistance groups throughout the countryside. Allied “Jedburg” teams, soldiers trained to aid the resistance, sabotage German supply lines, and unify the command of partisan groups, parachuted into France behind German lines. Individual Jedburg soldiers used the underground network to reach the towns or groups in which they were to operate. The two-way traffic of Allied servicemen in the “underground railroad” system facilitated communication not only with diverse resistance groups, but also with Allied command.

Jedburg groups also coordinated the procurement and allocation of radios to facilitate communication. While radios carried an increased risk of detection by occupation forces, they made mass communication over longer distance possible. Coded messages were transmitted nightly, both to Allied command and to various area partisans. Messages identified their recipients with a cryptonym and gave necessary instructions in coded messages. The codes were agreed upon in person, and then used in broadcasts

to activate plans. When intercepted, the messages were easily identifiable as partisan transmissions, but their meanings were indecipherable. British radio, and the European underground radio, often rebroadcast Jedburg and other resistance messages. While this coding method was primitive, it required German forces to use spies instead of technology as primary means of breaking resistance group communications. Such missions were a costly drain on human intelligence resources, and carried a high level of risk.

In 1944, many of the largest French underground groups united to form the *Conseil National de la resistance*. The organization stockpiled weapons and worked with Allied intelligence operatives to prepare for the Allied invasion of France. During the D-Day invasion in June, 1944, the resistance cut German supply lines and aided Allied forces as they marched through France. Urban partisan members in Paris took to the streets in open warfare against the Germans, engaging forces until the liberation of Paris. With the Allied invasion, exiled members of the French Army, under the command of Charles de Gaulle, returned to France. Many resistance members then joined the army, fighting enemy forces throughout Europe.

Over the course of the war, the French Resistance scored key victories against the German occupations forces. Resistance members tracked and ferreted-out French collaborators, assassinated many ranking Nazi officials, tapped the phones of the Abwehr’s Paris headquarters, and destroyed trains, convoys, and ships used by the German army. The resistance provided Allied forces with invaluable human intelligence resources and aided Allied troops who fell behind enemy lines. Resistance groups shielded political dissidents, refugees, and Jews escaping the Holocaust.

These numerous accomplishments carried a heavy price. German agents often infiltrated partisan groups, despite security precautions. When they captured a maquis, Gestapo agents employed torture as means of extracting the names of other resistance members. The Gestapo occasionally carried out bloody reprisals on innocent civilians after partisan sabotage operations. As many as 25,000 French men and women, members of the resistance and those suspected of aiding their cause, were sent to German concentration camps. Another 25,000 were executed in France by Gestapo agents, including the population of an entire Northern French village.

#### ■ FURTHER READING :

##### BOOKS:

- Aubrac, Lucie. Konrad Bieber and Betsy Wing (trans.). *Outwitting the Gestapo*. Lincoln: University of Nebraska Press, 1994.
- Aubrac, Raymond, and Lucie Aubrac. *The French Resistance: 1940–1944*. Paris: Hazan Editeur, 1997.

Ottis, Sherri Greene. *Silent Heroes: Downed Airmen and the French Underground*. Lexington, KY: University of Kentucky Press, 2001.

Osby, Ian. *Occupation*. Lanham, MD: Cooper Square Press, 2000.

Weitz, Margaret Collins. *Sisters in the Resistance : How Women Fought to Free France, 1940–1945*. New York: John Wiley & Sons., 1998.

## SEE ALSO

*France, Intelligence and Security*  
*OSS (United States Office of Strategic Services)*

---

# Fusion

---

Nuclear fusion is the process by which two light atomic nuclei combine to form one heavier atomic nucleus. As an example, a proton (the nucleus of a hydrogen atom) and a neutron will, under the proper circumstances, combine to form a deuteron (the nucleus of an atom of “heavy” hydrogen). In general, the mass of the heavier product nucleus is less than the total mass of the two lighter nuclei. Nuclear fusion is the initial driving process of nucleosynthesis.

The practical problems of building a fusion power plant are formidable, and the technology to construct a suitable containment vessel or field in which controlled fusion reactions could take place does not yet exist. Currently the only fusion reactions that take place on Earth are uncontrolled fusion reaction in nuclear weapons (e.g., H-bombs).

In April, 2003, Sandia scientists reported that they had achieved controlled thermonuclear fusion in a pulsed power source. If ultimately reproduced and verified, the process, and other competing approaches to controlled fusion, holds the promise of nearly unlimited clean power generation. Unlike fission reactions, fusion based energy technology would not produce long-lived radioactive waste.

Instead of using magnetic containment to compress hydrogen and thereby achieve temperatures hot enough for fusion to occur, Sandia scientists used pulsed releases of current to achieve a rapid series of limited micro fusion reactions. Using an improved and more powerful Z accelerator, high current is induced in a tungsten wire cage surrounding a 2 mm plastic capsule containing deuterium (an heavier isotope of hydrogen). The tungsten cage is vaporized, but the short-lived current impulse generated in the wires creates a powerful magnetic pulse and shockwave of superheated tungsten that creates an intense x-ray source that, along with the shockwave compresses and heats the hydrogen to more than 20 million degrees Fahrenheit (more than 11 million degrees Celsius) to induce fusion.

The Sandia reaction process contrasts with another promising approach undertaken at the Lawrence Livermore National Laboratory (LLNL) that seeks to initiate fusion reactions by shining high energy lasers on hydrogen globules. The LLNL approach will be further explored at the National Ignition Facility.

Scientists who worked on the first fission (atomic) bomb during World War II were aware of the potential for building an even more powerful bomb that operated on fusion principles. A fusion bomb uses a fission bomb as a trigger (a source of heat and pressure to create a fusion chain reaction. In the microseconds following a fission explosion fusion begins to occur within the casing surrounding the fission bomb. Protons, deuterons, and tritons begin fusing with each other, releasing more energy, and initiating other fusion reactions among other hydrogen isotopes.

**The fusion sequence.** When a proton and neutron combine, the mass of the resulting deuteron is 0.00239 atomic mass units (amu) less than the total mass of the proton and neutron combined. This “loss” of mass is expressed in the form of 2.23 MeV (million electron volts) of kinetic energy of the deuteron and other particles and as other forms of energy produced during the reaction. Nuclear fusion reactions are like nuclear fission reactions, therefore, in that some quantity of mass is transformed into energy. This is the reason stars “shine” (i.e., radiate tremendous amounts of electromagnetic energy into space).

The particles most commonly involved in nuclear fusion reactions include the proton, neutron, deuteron, a triton (a proton combined with two neutrons), a helium-3 nucleus (two protons combined with a neutron), and a helium-4 nucleus (two protons combined with two neutrons). Except for the neutron, all of these particles carry at least one positive electrical charge. That means that fusion reactions always require very large amounts of energy in order to overcome the force of repulsion between two like-charged particles. For example, in order to fuse two protons, enough energy must be provided to overcome the force of repulsion between the two positively charged particles.

As early as the 1930s, a number of physicists considered the possibility that nuclear fusion reactions might be the mechanism by which energy is generated in the stars. No familiar type of chemical reaction, such as combustion or oxidation, could possibly explain the vast amounts of energy released by even the smallest star. In 1939, the German-American physicist Hans Bethe worked out the mathematics of energy generation in which a proton first fuses with a carbon atom to form a nitrogen atom. The reaction then continues through a series of five more steps, the net result of which is that four protons are consumed in the generation of one helium atom.

Bethe chose this sequence of reactions because it requires less energy than does the direct fusion of four protons and, thus, is more likely to take place in a star.

Bethe was able to show that the total amount of energy released by this sequence of reactions was comparable to that which is actually observed in stars.

The Bethe carbon-cycle is by no means the only nuclear fusion reaction. A more direct approach, for example, would be one in which two protons fuse to form a deuteron. That deuteron could then fuse with a third proton to form a helium-3 nucleus. Finally, the helium-3 nucleus could fuse with a fourth proton to form a helium-4 nucleus. The net result of this sequence of reactions would be the combining of four protons (hydrogen nuclei) to form a single helium-4 nucleus. The only net difference between this reaction and Bethe's carbon cycle is the amount of energy involved in the overall set of reactions.

Other fusion reactions include D-D and D-T reactions. The former stands for deuterium-deuterium and involves the combination of two deuterium nuclei to form a helium-3 nucleus and a free neutron. The second reaction stands for deuterium-tritium and involves the combination of a deuterium nucleus and a tritium nucleus to produce a helium-4 nucleus and a free neutron.

The term "less energy" used to describe Bethe's choice of nuclear reactions is relative; however, since huge amounts of energy must be provided in order to bring about any kind of fusion reaction. In fact, the reason that fusion reactions can occur in stars is that the temperatures in their interiors are great enough to provide the energy needed to bring about fusion. Because those temperatures generally amount to a few million degrees, fusion reactions are also known as thermonuclear (thermo = heat) reactions. The heat to drive a thermonuclear reaction is created during the conversion of mass to energy during other thermonuclear reaction.

**Fusion bombs.** From a military standpoint, the fusion bomb had one powerful advantage over the fission bomb. For technical reasons, there is a limit to the size one can make a fission bomb. However, there is no technical limit on the size of a fusion bomb. One simply makes the casing surrounding the fission bomb larger. On August 20, 1953, the Soviet Union announced the detonation of the world's first fusion bomb. It was about 1,000 times more powerful than was the fission bomb that was dropped on Hiroshima less than a decade earlier. Since that date, both the Soviet Union (now Russia) and the United States have stockpiled thousands of fusion bombs and fusion missile warheads. The manufacture, maintenance, and destruction of these weapons remain a source of scientific and geopolitical debate.

**Possible peaceful uses for fusion.** As research on fusion weapons continued, attempts were also being made to develop peaceful uses for nuclear fusion. The containment vessel problems remain daunting because at the temperatures at which fusion occurs, known materials

vaporize instantly. Traditionally, two general approaches hold promise of possibly solving this problem: magnetic and inertial containment.

One way to control hot plasma is with a magnetic field. One can design such a field so that a swirling hot mass of plasma within it can be held in a specified shape. Other proposed methods of control include the use of suspended microballoons that are then bombarded by the laser, electron, or atomic beam to cause implosion. During implosion, enough energy is produced to initiate fusion.

The production of useful nuclear fusion energy depends on three factors: temperature, containment time, and energy release. That is, it is first necessary to raise the temperature of the fuel (the hydrogen isotopes) to a temperature of about 100 million degrees. Then, it is necessary to keep the fuel suspended at that temperature long enough for fusion to begin. Finally, some method must be found for tapping off the energy produced by fusion.

In late twentieth century, scientists began to explore approaches to fusion power that departed from magnetic and inertial confinement concepts. One such approach was called the PBFA process. In this machine, electric charge is allowed to accumulate in capacitors and then discharged in 40-nanosecond micropulses. Lithium ions are accelerated by means of these pulses and forced to collide with deuterium and tritium targets. Fusion among the lithium and hydrogen nuclei takes place, and energy is released. However, the PBFA approach to nuclear fusion has been no more successful than has that of more traditional methods.

In March of 1989, two University of Utah electrochemists, Stanley Pons and Martin Fleischmann, reported that they had obtained evidence for the occurrence of nuclear fusion at room temperatures (i.e., cold fusion). During the electrolysis of heavy water (deuterium oxide), it appeared that the fusion of deuterons was made possible by the presence of palladium electrodes used in the reaction. If such an observation could have been confirmed by other scientists, it would have been truly revolutionary. It would have meant that energy could be obtained from fusion reactions at moderate temperatures. The Pons-Fleischmann discovery was the subject of immediate and intense scrutiny by scientists around the world. It soon became apparent, however, that evidence for cold fusion could not consistently be obtained by other researchers. A number of alternative explanations were developed by scientists for the apparent fusion results that Pons and Fleischmann believed they had obtained and most researchers now assert that Pons and Fleischmann's report of "cold fusion" was an error and that the results reported were due to other chemical reactions that take place during the electrolysis of the heavy water.

In January 2003, the United States rejoined the International Fusion Program, an international effort to construct an experimental fusion reactor. Recent progress in

controlling plasmas and developing technologies for burning plasma reactors may eventually provide a workable containment system.

■ FURTHER READING:

BOOKS:

Boyd, T. J. M. and J. J. Anderson *The Physics of Plasma*.  
Cambridge, UK: Cambridge University Press, 2003.

ELECTRONIC:

United Kingdom Atomic Energy Authority. "Focus on Fusion." <<http://www.fusion.org.uk/focus/index.htm>> (March 29, 2003).

United States Department of Energy, Office of Fusion Energy Sciences. "Welcome to the U.S. Fusion Energy Sciences Program." <<http://www.fofe.er.doe.gov/>> (March 30, 2003).

SEE ALSO

*Nuclear Detection Devices*  
*Nuclear Weapons*  
*Radioactive Waste Storage*





## G-2

The term *G-2* refers to the intelligence staff of a unit in the United States Army. It is contrasted with *G-1* (personnel), *G-3* (operations), and *G-4* (supply). In the navy, these sections have their counterparts, each with an *N-* designation, while at the level of the Joint Staff, the sections use the prefix *J-*.

The *G-*system, as well as the basic structure of military intelligence and even the concept of an army general staff, are surprisingly modern creations. Although George Washington proved shrewd at gathering and using intelligence in the American Revolution, it was only in 1885 that the army formally instituted its Division of Military Information under the Adjutant General's Office.

European armies had meanwhile adopted the *G-*designations, which originated in France. In 1903, the U.S. Army implemented the concept of a permanent general staff, and with it the four sections pioneered in Europe. The Division of Military Information thus became *G-2*.

Interest in military intelligence grew during World War I, which saw the formation of an intelligence division under the War Department General Staff. The army also instituted the use of staffs that included intelligence officers all the way down to the battalion level. This emphasis on military intelligence, however, subsided after the armistice.

The army treated the work of *G-2* as a function that any officer could fill, hence there was no need for any permanent military intelligence organization. In 1950, General Dwight D. Eisenhower commented in an address to the War College, "I think that officers of ability in all our services shied away from the intelligence branch in the fear that they would be forming dimples in their knees by holding teacups in Buenos Aires or Timbuctoo."

Although the army had developed a Military Intelligence Division (MID) at the end of World War I, its resources were limited, even during World War II. At the same time, the war finally saw the transfer of signals intelligence from the signal corps to *G-2*. In a 1946 reorganization of the army, MID was placed over the Army Security Agency (ASA) and the Counter Intelligence Corps (CIC), but in contrast to this emphasis on signals intelligence, there was no command concerned with human and imagery intelligence.

Those demands would be met in the postwar era, which saw an explosion in the growth of *G-2* functions. Today, military intelligence is as critical a component of army operations as logistics, and it may seem difficult to imagine a time when commanders did not recognize that fact.

### ■ FURTHER READING:

#### BOOKS:

- Berkowitz, Bruce D., and Allan E. Goodman. *Strategic Intelligence for American National Security*. Princeton, NJ: Princeton University Press, 1989.
- Finnegan, John Patrick, and Romana Danysh. *Military Intelligence*. Washington, D.C.: Center of Military History, United States Army, 1998.
- Miller, Nathan. *Spying for America: The Hidden History of U.S. Intelligence*. New York: Paragon House, 1989.
- Suvorov, Viktor. *Inside Soviet Military Intelligence*. New York: Macmillan, 1984.

#### SEE ALSO

- Army Security Agency*
- INSCOM (United States Army Intelligence and Security Command)*
- Joint Chiefs of Staff, United States*

## Gamma Radiation Detectors.

SEE *Environmental Measurements Laboratory*.

## GAO (General Accounting Office, United States)

The United States General Accounting Office, or GAO, is an independent agency charged with investigating expenditures by the federal government, as well as activities associated with those expenditures. The GAO issues some 1,000 reports a year, and since September 2001, its evaluation of security measures undertaken by the federal government have provided a key means for assessing the degree to which various agencies and departments are prepared, or not prepared, for terrorist threats. The GAO, which reports directly to Congress, is known as the “congressional watchdog” for its role in overseeing federal spending of taxpayer dollars.

**The early GAO.** In the aftermath of World War I, government accounting and financial management was in a state of disarray. The war had brought unprecedented costs on the federal government, which had expanded considerably to accommodate its new role on the world stage, and Congress lacked adequate means of reviewing budgets and spending. To address the problem, in 1921, it passed the Budget and Accounting Act, which created GAO as an auditor independent of the executive branch.

The next major phase of government expansion attended the implementation of President Franklin D. Roosevelt’s New Deal during the 1930s, and GAO grew apace. Its workforce, including 1,700 employees in 1921, grew to 5,000 by 1940. With the coming of World War II, the size of government ballooned to proportions not seen even in World War I or the Great Depression, and the growth of GAO to 14,000 employees by 1945 reflected this. At the same time, GAO administrators found themselves unable to keep up with the ever-burgeoning paperwork, and this forced a reconsideration of GAO practices at war’s end.

**Reassessing its mission.** Prior to the end of World War II, the GAO had dutifully tracked every expenditure undertaken by the federal government, but by 1945 it had become clear that this practice was not working. GAO was awash in a sea of paper, and the minutiae of regular accounting had begun to obscure the larger picture of government finances. The agency therefore set about transferring some of its accounting functions, such as the checking of vouchers, to the executive branch of the federal government. Thereafter, its accounting role became more strategic than tactical. Instead of reviewing every expense sheet, the GAO began to oversee the financial control and management of federal agencies. In the late 1940s, it began to work with the Department of the Treasury and the Bureau of the Budget (which later became the Office of Management and Budget), assisting the agencies of the executive branch in improving their own accounting systems and

controls. It thus, delegated the more detailed tasks, and turned its attention to comprehensive auditing.

This reassessment of the GAO mission was reflected in reduction of its payroll to fewer than 7,000. The GAO, in fact, is one of the rare government agencies that actually decreased in size with the passage of time. Today its employees number about 3,300, including experts in program evaluation, law, accounting, economics, and other areas.

**The modern GAO.** Despite the reduction in its numbers, the GAO in the second half of the twentieth century expanded its operations commensurate with the growth of government that attended the early Cold War, the Great Society and War on Poverty, Vietnam, and later developments. The number of GAO offices around the country and around the world has expanded, as has the range of specialties among its employees. During the 1970s, GAO added scientists, actuaries, and specialists in fields such as health care, information systems, and public policy. In 1986, GAO developed its own team of professional investigators, many of whom have backgrounds in law enforcement.

Security and intelligence-related work has become increasingly important to the GAO mission, particularly in the atmosphere of heightened alert since the September 11, 2001 terrorist attacks upon the United States. The GAO has evaluated plans for the Department of Homeland Security and other measures undertaken in the wake of the terrorist attack, and has identified areas for improvement in many aspects of security at the local, state, or federal levels. In the fall 2002, for instance, the GAO reported that 13 of the hijackers involved in the September 11 incidents had not been interviewed by U.S. consular officials prior to the granting of visas. The GAO also evaluated the measures taken by 24 of the largest federal departments and agencies to protect their computers from fraud, misuse, or cyberterrorism, and found that 14 of these had failed to undertake appropriate measures for the protection of their information systems.

### ■ FURTHER READING:

#### BOOKS:

- Alexander, Yonah, and Michael S. Swetnam. *Cyber Terrorism*. Ardsley, NY: Transnational, 2001.
- Trask, Roger R. *Defender of the Public Interest: The General Accounting Office, 1921–1996*. Washington, D.C.: General Accounting Office, 1996.

#### PERIODICALS:

- Eggen, Dan. “Hijackers Got Visas with Little Scrutiny, GAO Reports.” *Washington Post*. (October 22, 2002): A7.

#### ELECTRONIC:

- Lee, Christopher. “Agencies Fail Cyber Test; Report Notes ‘Significant Weaknesses’ in Computer Security.” *Washington Post*. (November 20, 2002): A23.

General Accounting Office. <<http://www.gao.gov/>> (February 23, 2003).

#### SEE ALSO

*Counter-Intelligence*  
*Critical Infrastructure Assurance Office (CIAO), United States*  
*Cyber Security*  
*Intelligence, United States Congressional Oversight*  
*United States, Counter-Terrorism Policy*

## Gas Chromatograph-Mass Spectrometer

■ LAURIE DUNCAN

The gas chromatograph-mass spectrometer (GC/MS) is an instrument used to analyze the molecular and ionic composition of chemical compounds. GC/MS technology combines two widely used laboratory techniques: gas chromatography (GC), which separates and identifies compounds in complex mixtures, and mass spectrometry (MS), which determines the molecular weight and ionic components of individual compounds. The combination of these two powerful tools into a single instrument—the chemical separates produced by the gas chromatograph become the input for the mass spectrometer—allows for quick, precise analyses of solid, liquid and gaseous chemical compounds.

Scientists from a wide range of fields currently use GC/MS to identify and analyze inorganic, organic, and bio-organic chemicals. Academic researchers have long used either gas chromatography or mass spectrometry to assess experimental outcomes, analyze biochemical reactions, and age-date geological samples; many of these theoretical and experimental scientists have adopted the newer, more precise, and faster GC/MS technology to replace the two separate instruments. Industrial applications of GC/MS include pharmaceutical drug discovery and testing, process monitoring in the petroleum, chemical, and pharmaceutical industries, and identification of unknown chemicals in applied forensic, military, and environmental sciences.

Gas chromatography is a technique for separating closely-related compounds (solutes) from a liquid or gaseous mixture. (Solids must be vaporized or liquefied before analysis.) GC is most commonly used to separate and detect volatile and semi-volatile organic compounds (VOCs and SVOCs) with molecular weights less than 500 atomic mass units (amu). Although chemists have probably used

rudimentary chromatography to separate mixtures since the Middle Ages, the modern chromatograph was not developed until 1941 when British biochemists Archer Martin and Richard Synge invented a chromatographic method that allowed for precise partitioning and detection. Martin and Synge were awarded the 1952 Nobel Prize in chemistry for their efforts.

The GC component of a GC/MS system includes a carrier gas supply, a sample introduction inlet, a capillary column coated with a stationary liquid or solid, and an outlet to the detection system, in this case a mass spectrometer. To begin analysis, a GC/MS technician vaporizes the sample, or analyte, and introduces it into the chromatograph by syringe injection through a rubber septum. A flow of inert carrier gas like helium, argon, or nitrogen moves the analyte into the separation column. Partitioning occurs as the gaseous components of the original analyte assume different velocities when confronted with the column's liquid or solid coating. Partitioning behavior is temperature-dependent, and precise temperature control is an important part of the GC process. A filter removes the separated compounds from the carrier gas at the end of the column before they are fed into the mass spectrometer for individual analysis.

Mass spectrometry is a method of determining the molecular weights of a chemical compound's component ions. (Ions are electrically charged atoms or groups of atoms, and sub-particles of molecules.) The MS instrument, known as the "smallest scale in the world", provides a graph, or mass spectrum, with peaks that indicate the relative amount of each type of ion within a compound. Today's MS systems are based on Sir J. J. Thomson's research at the Cavendish Laboratory at the University of Cambridge. Thomson discovered the electron in 1897, and went on to observe that the parabolic paths of ions traveling through electrical and magnetic fields vary according to the ions' mass-to-charge ( $m/z$ ) ratios. His experimental instruments were the first mass spectrometers, and he was awarded the 1906 Nobel Prize in physics for his discoveries.

MS instrumentation has become increasingly accurate and complex since Thomson's time, but the principles of the technique and its basic components have remained the same. The MS component of a GC/MS system includes a sample inlet into a vacuum-sealed chamber that houses an ionization source, a mass analyzer, and an ion detector. In a GC/MS system the input sample is always a chemically homogenous gas produced by the GC component that can be introduced directly to the ionizer. Once ionized, the partitioned compound moves into the mass analyzer where the ions travel through an electrical or magnetic field that sorts them according to their  $m/z$  ratios. The detector measures the beam of now-separated ions arriving at the end of the analyzer, and converts changes in its intensity to produce the mass spectrum. A sample's mass spectrum is then displayed, catalogued, and compared to a library of known mass spectra by a computer data



A researcher at the Environmental Technology Group at Pennsylvania State University holds a Suma canister, a device used to collect air samples, in front of a cryogenic concentrator and gas chromatograph that is used to analyze the sample. AP/WIDE WORLD PHOTOS.

system. For many applications, environmental monitoring or drug testing at sporting events, for examples, an unknown sample can be identified using a fairly short list of possible spectra. Other applications, like theoretical chemistry, organic chemistry, or planetary exploration may require an enormous library of possible molecules for identification, and may even produce previously unknown molecules.

Improvements in the individual GC and MS components, electronic automation, and computer data analysis and storage have led to machines that can analyze ever more complex, fragile, and tiny chemical components; GC/MS can now be used to quickly analyze proteins, DNA, and even viruses, and has become a common technique in molecular biology and medical science. GC/MS instruments are also becoming smaller and less expensive, and field laboratory and even portable, suitcase-sized systems that can be used to analyze forensic samples, environmental contaminants, and unknown agents of chemical and biological warfare on site now exist. Remotely operated GC/MS systems are planned components of future space exploration expeditions that hope to characterize the chemical makeup of extra-terrestrial environments, and to search for organic material elsewhere in our solar system.

#### ■ FURTHER READING:

##### ELECTRONIC:

Massachusetts Institute of Technology. "Present Life: Spectroscopic Analysis Gas Chromatography/Mass Spectrometry (GC/MS)." Mars Mission 2004, student final presentation. December 10, 2000. <<http://web.mit.edu/12.000/www/finalpresentation/experiments/index.html>> (January 5, 2003).

Scripps Center for Mass Spectrometry (BC-007), 10550 North Torrey Pines Rd., La Jolla, CA 92037. (858) 784-9596. Gary Suizdak, director. <<http://masspec.scripps.edu/information/intro/index.html>> (January 5, 2003).

Signature Science, LLC8329 North Mopac Blvd Austin, TX 78759. (512) 533-2022. Cassandra Hutson, staff chemist. <<http://www.signaturescience.com>> (January 8, 2003).

United States Environmental Protection Agency. "Technology: Gas Chromatography." January 2001. <<http://fate.clu-in.org/gc.asp?techtypeid=44>> (January 9, 2003).

##### SEE ALSO

*Air Plume and Chemical Analysis*

*Biological Warfare*

*Isotopic Analysis*

*Microbiology: Applications to Espionage, Intelligence and Security*

## General Services Administration, United States

The General Services Administration (GSA) is one of the three central management agencies of the federal government, along with the Office of Personnel Management and the Office of Management and Budget. It affects almost \$66 billion in federal spending, or about a quarter of total procurement dollars at the government's disposal, and manages assets collectively valued at almost \$500 billion. Its mission is to support federal employees by securing the buildings, equipment, and property they need.

**Early roles.** GSA was the result of a study conducted in the 1940s by a commission under the direction of President Herbert Hoover. Charged with developing a means to enhance the effectiveness of administrative services provided by the federal government, the Hoover Commission recommended that the government disband four small agencies and consolidate them into a single large office. The result was GSA, created by the Federal Property and Administrative Services Act, which President Harry S. Truman signed into law on July 1, 1949.

The functions of the early GSA included many retained by the agency today, as well as others that have either fallen by the wayside or been transferred to other parts of the federal government. It oversaw emergency management functions that were transferred to the Federal Emergency Management Agency in 1979; kept national archives that were moved to the National Archives and Records Administration in 1985; and stockpiled strategic materials that would be in short supply during wartime, a function given over to the Department of Defense in 1988.

**GSA and government infrastructure.** GSA in the early years also had a number of exotic roles, including management of hemp plantations in South America. On the other hand, the first two decades of GSA's life also saw the introduction of operations that would become integral to its mission over the years that followed. In 1954, GSA established the first federal motor pool, and in 1959 created the Federal Procurement Regulation System. In the early 1960s GSA—which in 1957 had been the first federal agency to use the term “telecommunication system”—initiated the federal intercity telecommunications system.

In 1962, a GSA committee recommended to President John F. Kennedy that a number of government buildings in Washington, D.C., needed to be updated or replaced, and thus began a massive federal construction program. Ten years later, in 1972, GSA established the Federal Buildings Fund to pay for the maintenance, operation, renovation, and construction of federal buildings through the rental income paid to GSA by federal tenants.

One of the most visible aspects of GSA as it relates to the public appeared in 1970, with the establishment of the Consumer Information Center, whose many pamphlets and television commercials made its Pueblo, Colorado, distribution center famous around the country. In 1972, the agency created its Automated Data and Telecommunications Service, today known as the Federal Technology Service. GSA in 1984 began issuing its own credit cards, which federal employees use for small work-related purchases, as well as travel expenses. GSA opened its first child care center in 1987, and by the beginning of the twenty-first century managed some 111 centers in which 7,600 children of government employees were cared for while their parents worked—often in the same building.

Beginning with the creation of the Office of Federal Management Policy in 1973, GSA acquired a number of policymaking functions, which in 1995 were consolidated in the Office of Government-wide Policy. GSA in the 1990s was a leading proponent of new technology and practices, encouraging the use of telecommuting and introducing government employees to both the Internet and intranets.

**GSA today.** Among the most important of GSA's functions is its role in new government construction, which gained an added security dimension in the wake of the 1995 Oklahoma City bombings. As a result, GSA undertook a series of studies directed toward ensuring increased security for buildings. By the time of the 2001 terrorist incidents, GSA had begun to put some of these recommendations into place. For example, the portion of the Pentagon damaged by terrorists on September 11, 2001 had been recently remodeled with new measures in mind, a factor that probably saved a number of lives.

In its Design Excellence Program, GSA has worked with a number of leading architects from the private sector on public buildings ranging from courthouses—it has built or renovated court facilities in some 160 locations since the mid-1990s—to the Ronald Reagan Building and the International Trade Center. GSA also manages security in many of the more than 8,300 government-owned or -leased buildings it manages.

Today GSA controls a fleet of some 170,000 vehicles, and manages information technology products ranging from laptop computers to vast computer systems. The majority of its operating funds come from rental of the products, services, and properties it provides, and only one percent of its budget comes through congressional appropriations.

### ■ FURTHER READING:

#### BOOKS:

U.S. Government Printing Office. *Portals and Related Matters: Evidence Warranting Further Action by Federal*

*Enforcement Authorities*. Washington, D.C.: U.S. Government Printing Office, 1999.

#### PERIODICALS:

Ballard, Tanya N. "Horror, then a Helping Hand." *Government Executive* 33, no. 13 (October 2001): 12–14.

Grant, Peter. "Plots & Ploys." *Wall Street Journal*. (December 26, 2001): B4.

"RAMPART Assesses Threats." *Signal* 56, no. 1 (September 2001): 7.

Williams, Krissah. "U.S. Seeks to Build Secure Online Network." *Washington Post*. (October 11, 2001): A10.

#### ELECTRONIC:

General Services Administration. <<http://www.gsa.gov/>> (February 23, 2003).

#### SEE ALSO

*Architecture and Structural Security*  
*Critical Infrastructure*  
*Facility Security*

---

## Genetic Code

---

Although the genetic code is not a "code" in the sense normally used in intelligence and espionage terminology, a fundamental understanding of the genetic code is essential to understanding the molecular basis of advanced DNA and genetic tests that are increasingly important in forensic science and identification technology.

The genetic information that is passed on from parent to offspring is carried by the DNA of a cell. The genes on the DNA code for specific proteins that determine appearance, different facets of personality, health etc. In order for the genes to produce the proteins, it must first be transcribed from DNA to RNA in a process known as transcription. Thus, transcription is defined as the transfer of genetic information from the DNA to the RNA. Translation is the process in which genetic information, carried by messenger RNA (mRNA), directs the synthesis of proteins from amino acids, whereby the primary structure of the protein is determined by the nucleotide sequence in the mRNA.

The genetic code is the set of correspondences between the nucleotide sequences of nucleic acids such as deoxyribonucleic acid (DNA), and the amino acid sequences of proteins (polypeptides). These correspondences enable the information encoded in the chemical components of DNA to be transferred to the ribonucleic acid messenger (mRNA) and then used to establish the correct sequence of amino acids in the polypeptide. The elements of the encoding system, the nucleotides, differ by only four

different bases. These are known as adenine (A), guanine (G), thymine (T) and cytosine (C), in DNA or uracil (U) in RNA. Thus RNA contains U in the place of C and the nucleotide sequence of DNA acts as a template for the synthesis of a complementary sequence of RNA, a process known as transcription. For historical reasons, the term genetic code in fact refers specifically to the sequence of nucleotides in mRNA, although today it is sometimes used interchangeably with the coded information in DNA.

Proteins found in nature consist of 20 naturally occurring amino acids. One important question is, how can four nucleotides code for 20 amino acids? This question was raised by scientists in the 1950s soon after the discovery that the DNA comprised the hereditary material of living organisms. It was reasoned that if a single nucleotide coded for one amino acid, then only four amino acids could be provided for. Alternatively, if two nucleotides specified one amino acid, then there could be a maximum number of 16 (4<sup>2</sup>) possible arrangements. If, however, three nucleotides coded for one amino acid, then there would be 64 (4<sup>3</sup>) possible permutations, more than enough to account for all the 20 naturally occurring amino acids. The latter suggestion was proposed by the Russian born physicist, George Gamow (1904–1968) and was later proved to be correct. It is now well known that every amino acid is coded by at least one nucleotide triplet or codon, and that some triplet combinations function as instructions for the termination or initiation of translation. Three combinations in tRNA, UAA, UGA and UAG, are termination codons, while AUG is a translation start codon.

The genetic code was solved between 1961 and 1963. The American scientist Marshall Nirenberg (1927–), working with his colleague Heinrich Matthaei, made the first breakthrough when they discovered how to make synthetic mRNA. They found that if the nucleotides of RNA carrying the four bases A, G, C and U, were mixed in the presence of the enzyme polynucleotide phosphorylase, a single stranded RNA was formed in the reaction, with the nucleotides being incorporated at random. This offered the possibility of creating specific mRNA sequences and then seeing which amino acids they would specify. The first synthetic mRNA polymer obtained contained only uracil (U) and when mixed *in vitro* with the protein synthesizing machinery of *Escherichia coli* it produced a polyphenylalanine—a string of phenylalanine. From this it was concluded that the triplet UUU coded for phenylalanine. Similarly, a pure cytosine (C) RNA polymer produced only the amino acid proline, so the corresponding codon for cytosine had to be CCC. This type of analysis was refined when nucleotides were mixed in different proportions in the synthetic mRNA and a statistical analysis was used to determine the amino acids produced. It was quickly found that a particular amino acid could be specified by more than one codon. Thus, the amino acid serine could be produced from any one of the combinations UCU, UCC, UCA, or UCG. In this way the genetic code is said to be degenerate, meaning that each of the 64 possible triplets



Genetic testing showed that this skull belonged to Martin Bormann, Hitler's private secretary. Bormann, who was missing and sentenced in absentia for war crimes at the Nuremberg trials of 1946, is shown in the photo at right. AP/WIDE WORLD PHOTOS.

have some meaning within the code and that several codons may encode a single amino acid.

This work confirmed the ideas of the British scientists Francis Crick (1916–) and Sydney Brenner (1927–). Brenner and Crick were working with mutations in the bacterial virus bacteriophage T4 and found that the deletion of a single nucleotide could abolish the function of a specific gene. However, a second mutation in which a nucleotide was inserted at a different, but nearby position, restored the function of that gene. These two mutations are said to be suppressors of each other, meaning that they cancel each other's mutant properties. It was concluded from this that the genetic code was read in a sequential manner starting from a fixed point in the gene. The insertion or deletion of a nucleotide shifted the reading frame in which succeeding nucleotides were read as codons, and was thus termed a frameshift mutation. It was also found that whereas two closely spaced deletions, or two closely

spaced insertions, could not suppress each other, three closely spaced deletions or insertions could do so. Consequently, these observations established the triplet nature of the genetic code. The reading frame of a sequence is the way in which the sequence is divided into the triplets and is determined by the precise point at which translation is initiated. For example, the sequence CATCATCAT can be read CAT CAT CAT or C ATC ATC AT or CA TCA TCA T in the three possible reading frames. Sometimes, as in particular bacterial viruses, genes have been found that are contained within other genes. These are translated in different reading frames so the amino acid sequences of the proteins encoded by them are different. Such economy of genetic material is, however, quite rare.

The same genetic code appears to operate in all living things, but exceptions to this universality are known. In human mitochondrial mRNA, AGA and AGG are termination or stop codons. Other differences also exist in the

correspondences between certain codon sequences and amino acids.

#### ■ FURTHER READING :

##### BOOKS:

Brenner, Sydney. *My Life in Science*. London: BioMed Central, Ltd., 2001.

Davies, Kevin. *Cracking The Genome: Inside The Race To Unlock Human DNA*. New York: Free Press, 2001.

Watson, James D. *The Double Helix: A Personal Account of the Discovery of the Structure of DNA*. Westport, CT: Touchstone Books, 2001.

———. *DNA: The Secret of Life*. New York: Knopf, 2003.

##### SEE ALSO

*DNA Fingerprinting*

*Forensic Science*

*Genetic Information: Ethics, Privacy, and Security Issues*

*Genetic Technology*

*Genomics*

## Genetic Fingerprinting.

SEE *DNA Fingerprinting*.

## Genetic Identification.

SEE *Sequencing*.

## Genetic Imagery Exploitation (GENIE).

SEE *Los Alamos National Laboratory*.

# Genetic Information: Ethics, Privacy, and Security Issues

■ CONSTANCE K. STEIN

Genetic information refers to all of the known genetic data for all organisms, but it can also refer to the genetic makeup of one individual or one family. Initially, genetics was highly statistical and relied on the expression of particular characters in various family members to determine a pattern of inheritance and estimate risks of recurrence. However, the field has become much more complicated

with the accumulation of data on over 10,000 genes that have been associated with human disease or phenotypic variation. It is now possible to identify individuals using genetic markers (DNA fingerprinting) and to predict with relative confidence that certain persons will have particular genetic diseases or features while others will be disease free. The data collected have improved diagnosis and treatment of some diseases, but this has also led to a series of ethical, privacy and security issues including concerns about what types of genetic testing are necessary, who should have access to the information after the testing is complete, and how that information should be used.

One of the great benefits of genetics has been the ability to uniquely identify individuals. In criminal cases, it is now possible to examine a crime scene specimen and directly connect it to a suspect. Molecular genetic technologies have also proven useful in the identification of human remains from plane crashes, the World Trade Center disaster, and a set of bones from the Tomb of the Unknown Soldier. Genetic identification has proven so robust that the United States Armed Forces now routinely maintains genetic profiles on all service personnel to facilitate identification. In addition, some metropolitan police units are offering DNA identity testing for children if the parents wish to have profiles of their children placed in a database in case of a future tragedy.

Whenever such genetic information is collected and stored, the issue of security becomes paramount. Databases must be very secure, and only authorized individuals should access the data, and then only with subject consent and when it's absolutely necessary. Password protection, restricted access, and encryption of data may be employed to assure confidentiality. It is also possible to set up a coding system whereby an individual's name is assigned a code, and the genetic results are only linked to the code number. The code and the key list must then be filed in separate secure locations.

Ethical considerations have also multiplied with the increase in genetics knowledge. Although it is now often possible to tell an individual that he or she will have a genetic disease, that person may not want to know that information. The primary concerns regarding genetic testing are both social and financial. Many people are frightened that a positive finding on a genetic test will result in discrimination and ostracism because they will be considered abnormal. There is also a very real concern that genetic test information may result in loss of or inability to get insurance or a job. Another issue is quality of life. If a test is done on a 20 year old who is then told that he or she will have a debilitating disease starting about the age of 45, how will that affect him or her psychologically? Regarding personal autonomy, should children be tested for late onset diseases or should testing be delayed until an individual is old enough to make his or her own decision about it? Because genetic diseases are typically inherited, identification of a disease causing mutation in one person may



mean that other family members are at risk for the disease. Should genetic information be shared within families, and, if so, how should that be accomplished keeping an individual's autonomy in mind? Should prenatal genetic testing be done, and if a mutation for a deleterious disease is found, how should that pregnancy be handled? For serious diseases, should population-screening tests be mandated so that affected individuals are recognized and appropriate treatment can be rendered? Should population screening be done for all identifiable diseases or only those for which treatment is available?

At the present time, there is no one answer to any of these very difficult ethical questions. Each person must approach the problem in his or her own way. Most experts agree that a person's genetic information should be private, and that, following counseling to explain the reason for and consequences of the test in question, individuals should be allowed to choose when and which tests are done and with whom the results are shared. Only tests of proven reliability and significance should be performed, and results should be interpreted and utilized by trained personnel. Tests for late onset diseases are usually restricted to persons old enough to understand the ramifications of the assay and the disease. The number and type of population screening tests currently being done is limited and only involves those diseases for which some type of treatment is available. These principles continue to be tested as new genes are identified, and the use of genetic information becomes increasingly important in diagnosis.

The next challenge is to keep all of the information collected confidential. A standard "release of medical information" will include the results of genetic tests as one element of the total package. Insurance companies frequently review a person's medical records before issuing a policy, but individuals with documented genetic disorders are considered high risks, and, so could be refused coverage. Employers may also decline to hire someone with a genetic "defect", fearing the employee may not be able to do the job. Alternatively, a genetic disease that does not affect a person's performance may still be a liability by increasing the health insurance premiums for everyone in the group policy. Recent new legislation has provided some protection against wholesale release of medical information, but this is not foolproof, and it is still possible for genetic data to get into the wrong hands. It has been suggested that some form of socialized medicine in the United States may be needed to give everyone equal protection and reduce the negative impact of a genetic diagnosis.

One final area of concern is research. Although the Human Genome Project has been completed, researchers are now attempting to isolate all of the genes present, determine their function, and identify mutations that lead to disease. Currently, individuals with rare diseases are recruited to participate in studies aimed at finding their disease gene, developing drugs to treat that disease, and testing those drugs for efficacy. In order to protect against

the unauthorized use of patient samples or the release of sensitive genetic information, the United States Code of Federal Regulations has established guidelines that are overseen by the Office for Human Research Protection. All participants must sign an informed consent, and specimens must be either anonymized or a coding system must be set up so that subjects and their genetic results cannot be easily connected. As a result, research protocols tend to have a very high level of security for their data.

Education may be the single most helpful tool in alleviating the concerns that surround the storage and use of genetic information. As the public becomes more aware of genetic principles, misunderstandings and misuse are lessening. Genetic counseling and access to the Internet are proving to be extremely valuable methods of providing the needed pieces of information.

#### ■ FURTHER READING:

##### BOOKS:

Nussbaum, R. L., R. R. McInnes, and H. F. Willard. *Thompson and Thompson Genetics in Medicine*, Sixth Edition. Philadelphia: Saunders, 2001.

##### PERIODICALS:

Collins, F. S., and V. A. McKusick. "Implementation of the Human Genome Project for Medical Science." *Journal of the American Medical Association* no. 285 (7) (2001): 540-544.

Gerard, S., M. Hayes, and M. A. Rothstein. "On the Edge of Tomorrow: Fitting Genomics Into Public Health Policy." *Journal of Law, Medicine and Ethics* no. 30 (3 Suppl) (2002): 173-176.

Jeffers, B. R. "Human Biological Materials in Research: Ethical Issues and the Role of Stewardship in Minimizing Research Risks." *Advances in Nursing Science* no. 24 (2) (2001): 32-46.

Khoury, M. J., L. L. McCabe, and E. R. B. McCabe. "Genomic Medicine: Population Screening in the Age of Genomic Medicine." *The New England Journal of Medicine* no. 348 (1) (2003): 50-58.

Nowlan, W. "A Rational View of Insurance and Genetic Discrimination." *Science* no. 297 (5579) (2002): 195-196.

Rothenberg, K. H., S. F. Terry. "Before It's Too Late—Addressing Fear of Genetic Information." *Science*. no. 297(5579) (2002): 196-197.

##### ELECTRONIC:

The Office of Human Research Protection. U.S. Department of Health and Human Services. April 14, 2003 <<http://ohrp.osophs.dhhs.gov>> (April 18, 2003).

Online Mendelian Inheritance in Man, OMIM (TM). McKusick-Nathans Institute for Genetic Medicine, Johns Hopkins University (Baltimore, MD) and National Center for Biotechnology Information, National Library of Medicine (Bethesda, MD), 2000. <<http://www.ncbi.nlm.nih.gov/omim/>> (April 18, 2003).

##### SEE ALSO

*DNA Fingerprinting*

*DNA Sequences, Unique  
Forensic Science  
Genomics*

*Health and Human Services Department, United States  
Molecular Biology: Applications to Espionage, Intelligence  
and Security*

---

## Genetic Technology

---

■ BRYAN COBB

Deoxyribonucleic acid (DNA), or an organism's genetic material—inherited from one generation to the next—holds many clues that have unlocked some of the mysteries behind human behavior, disease, evolution, and aging. As technological advances lead to a better understanding of DNA, new DNA-based genetic technologies will emerge. Recent advances in genetic and DNA technology, including cloning, PCR, recombinant DNA technology, DNA fingerprinting, gene therapy, DNA microarray technology, and DNA profiling, have already begun to shape medicine, forensic sciences, environmental sciences, and national security.

In 1956, the structure and composition of DNA was elucidated and confirmed previous studies more than a decade earlier demonstrating DNA is the genetic material that is passed down from one generation to the next. A novel tool called PCR (polymerase chain reaction) was developed not long after DNA was discovered. PCR represents one of the most significant discoveries or inventions in DNA technology and it led to a 1993 Nobel Prize award for American born Kary Mullis (1949–).

PCR is the amplification of a specific sequence of DNA so that it can be analyzed by scientists. Amplification is important, particularly when it is necessary to analyze a small sequence of DNA in quantities that are large enough to perform other molecular analyses such as DNA sequencing. Not long after PCR technology was developed, genetic engineering of DNA through recombinant DNA technology quickly became possible. Recombinant DNA is DNA that has been altered using bacterial derived enzymes called restriction endonucleases that act like scissors to cut DNA. The pattern that is cut can be matched to a pattern cut by the same enzymes from a different DNA sequence. The sticky ends that are created bind to each other and a DNA sequence can therefore be inserted into another DNA sequence.

Restriction endonucleases are also important in genetic fingerprinting. In this case, enzymes that recognize specific DNA sequences can produce fragments of DNA by cutting different parts of a long strand of DNA. If there are differences in the sequence due to inherited variation—meaning that there are extra DNA or specific sequences altered such that the restriction enzymes no

longer recognize the site, variable patterns can be produced. If these patterns are used to compare two different people, they will have a different fragment pattern or fingerprint. Genetic fingerprinting can be used to test for paternity. In forensics, genetic fingerprinting can be used to identify a criminal based on whether the person's unique DNA sequence matches to DNA extracted from a crime scene. This technology can also allow researchers to produce genetic maps of chromosomes based on these restriction enzyme fingerprints. Because there are many different enzymes, many different fingerprints can be ascertained.

Recombinant DNA technology can also be applied to splicing genes into molecular devices that can transport these genes to various cellular destinations. This technique, also called gene therapy, has been used to deliver corrected genes into individuals who have defective genes that cause disease. Gene splicing has also been applied to the environment as well. Various bacteria have been genetically modified to produce proteins that break down harmful chemical contaminants such as DDT. Currently, scientists are investigating the application of this technology to produce genetically engineered plants and crops that can produce substances that kill insects. Similarly, fruits can be engineered to have genes that produce proteins that slow the ripening process in an effort to extend their shelf life.

DNA microarray technology, also known as the DNA chip, is the latest in nanotechnology that allows researchers to study the genome in a high throughput manner. It can be used for gene expression profiling which gives scientists insights into what genes are being up or down-regulated. Various genetic profiles can be determined in order to estimate cancer risk or to identify markers that may be associated with disease. It has the ability only to detect changes in gene expression that are large enough to be detected above a baseline level. Therefore, it does not detect subtle changes in gene expression that might cause disease or play a role in the development of disease. It can also be used for genotyping, although clinical diagnostic genotyping using microarray technology is still being investigated.

Genes from other species can also be used to add new traits to a particular organism. For example, bacteria, mice, and plants have all had luminescent (light glowing) genes from jelly fish added to their genomes. Another reason for adding genes to a foreign organism is to manufacture various nutritional or pharmaceutical products. Some cows have been modified so that they can produce human insulin or vitamins in their milk in bulk. Pigs have been modified to overcome a number of transplantation problems so that some limited transplantation of organs can be carried out from pigs to humans, also called xenotransplantation.

DNA technology is a relatively new area of research with enormous controversy. It will likely continue to be a large part of public debate and have an impact on every

aspect of medical diagnostics, therapeutics, forensics, genetic profiling, and potential weapons development.

#### ■ FURTHER READING:

##### BOOKS:

Nussbaum, Robert L., Roderick R. McInnes, and Huntington F. Willard. *Genetics in Medicine*. Philadelphia: Saunders, 2001.

Rimoin, David L. *Emery and Rimoin's Principles and Practice of Medical Genetics*. London; New York: Churchill Livingstone, 2002.

##### SEE ALSO

*Biological Weapons, Genetic Identification*  
*DNA Recognition Instruments*  
*DNA Sequences, Unique*  
*Genomics*

## Genetrix Balloons.

SEE *U-2 Spy Plane*.

## GENIE (Genetic Imagery Exploitation).

SEE *Los Alamos National Laboratory*.

---

# Genomics

---

#### ■ JULI BERWALD

Genomics is the study of genes and their function in relation to the environment. In contrast to genetics, which focuses on genes and inheritance, the goal of genomics is to understand genes, their products and how, when, and why these products are synthesized.

The genome of every organism is the collection of the genetic information contained in the DNA (deoxyribonucleic acid). DNA is a molecule consisting of long strands of four different molecules called nucleotides: adenine, cytosine, guanine and thymine or A, C, G and T, as they appear in published sequences. The strands of DNA are paired so that A on one strand always corresponds to T on the opposite strand and similarly, C always corresponds to G. These paired strands of DNA are further twisted into the conformation of a double helix. A functional unit of DNA is called a gene. In a gene, the sequence of A, C, G, and T on a strand of DNA specifies the sequence of amino acids that make up a protein. In order for a specific protein to be synthesized, the DNA in a gene is first transcribed to messenger RNA (ribonucleic acid), which is similar to

DNA, but single stranded. The messenger RNA is then translated into a sequence of amino acids. In this process, three nucleotides of DNA, for example CGT, are transcribed into three nucleotides of messenger RNA, in this case GCA, which code for one amino acid, in this case alanine. Proteins and products of proteins are fundamentally responsible for all cellular behavior. Protein function is altered by changes in the sequence of amino acids. Genomics investigates how variations in genes affect protein structure and function throughout the life of a cell.

**The field of genomics.** Although it is a young and evolving field, genomics generally includes at least three key research areas: bioinformatics, proteomics and structural genomics. Masses of DNA sequence data have accumulated through projects like the Human Genome Project, the Mouse Genome Project and over 40 microbial genomes have been sequenced. Not all DNA is made up of genes. In humans, for example, only about 3% of the DNA is actually genes. Some of this non-coding DNA is used by enzymes as markers indicating the beginning and ends of genes. Some of it, the so-called junk DNA, may not have any function at all. Using statistical tools and data-mining techniques, the field of bioinformatics attempts to identify genes in the DNA and to determine the relationships among genes in different individuals. Although the DNA in organisms is essentially constant throughout their lives, the kinds and amounts of proteins that are synthesized at any instant are subject to much variation. The field of proteomics investigates which proteins are expressed at what stages in an organism's life and exactly how and why these proteins are expressed. Translating a sequence of DNA to its corresponding amino acid sequence is only the beginning of understanding the function of a protein. Many amino acid chains are modified after they are synthesized and protein structure changes depending on environmental conditions, e.g. heat, pH or association with other molecules. The study of structural genomics attempts to unravel the molecular structures that result from a sequence of DNA.

**Applications of genomics.** One of the most promising applications of genomics is improving the ability to fight diseases. Many diseases, such as sickle cell anemia, cystic fibrosis and Huntington's disease, are caused by abnormalities in the sequence of DNA that codes for a specific protein or proteins. Genomics will be able to help in both the diagnosis of these diseases and the treatment of these conditions. It is estimated that only about 500 molecules are actually targeted by drugs currently available. Genomics will hopefully lead to an increase in the number of drug targets used in pharmaceuticals. It may also provide information on the genetic basis for side effects and the effectiveness of treatments that can be used to tailor prescriptions for individuals. Two specific types of gene therapies have been advanced. Somatic cell therapy involves the insertion of therapeutic genes into specific cells in the body. This will hopefully allow those cells to synthesize

proteins that they are unable to produce or to turn off genes that are overexpressed. Germ line therapy involves the insertion of normal genes into an egg cell, with the hope that the normal gene will be incorporated in to the genome of the offspring and that a genetic disease will not be inherited.

In addition to their importance in medicine, bacteria, viruses and fungi play key roles in agriculture. Because their genomes are small, the genomes of at least 40 species of microorganisms have been sequenced. Understanding the genomics of these organisms has the potential to improve crop yields, decrease damage done by pest species and increase the nutritional value of food. As part of their metabolism, some microorganisms have the ability to break down harmful products and to produce energy as a product. Understanding the gene products involved in these transformations may lead to industrial uses, with the potential for solving different types of environmental problems and providing new energy sources.

**Military uses of genomics.** Identifying the genes and gene products in the organisms that lead to disease in humans will lead to the development of treatments for these diseases. Characterizing genes responsible for diseases will likely lead to the development of new antibiotics and other drugs used to treat diseases caused by biological warfare. It can also reveal methods for combating drug resistance and preventing the use of this phenomenon by opponents. Genomics should also provide new techniques for identifying biological agents on the battlefield. One of the most promising technologies is the biochip or DNA chip, which is a microarray of molecular probes on a silicon chip that specifically bind to the DNA of biological threats. Once bound, the DNA is then detected using a fluorescent signal. These arrays identify genes that are active in cells, and indicate if a particular immune response is occurring. In the case of a biological attack, this can provide quick, detailed information about the course of the infection to medical personnel.

#### ■ FURTHER READING:

##### ELECTRONIC:

American Medical Association. "Proteomics." <<http://www.ama-assn.org/ama/pub/category/3668.html#3>> (April 3, 2003).

Human Genome Project. "From the Genome to the Proteome." <[http://www.ornl.gov/TechResources/Human\\_Genome/project/info.html](http://www.ornl.gov/TechResources/Human_Genome/project/info.html)> (March 14, 2003).

Pharmaceutical Researchers and Manufacturers of America. "Genomics: A Global Resource." <<http://genomics.phrma.org/>> (April 3, 2003).

U.S. Department of Energy Joint Genome Institute. "An Introduction to Genomics." <[http://www.jgi.doe.gov/education/genomics\\_1.html](http://www.jgi.doe.gov/education/genomics_1.html)> (April 3, 2003).

Weizmann Institute of Science Genome and Informatics. <[http://bip.weizmann.ac.il/mb/functional\\_genomics.html](http://bip.weizmann.ac.il/mb/functional_genomics.html)> (April 3, 2003).

#### SEE ALSO

*Pathogen Genomic Sequencing*

## Geologic and Topographical Influences on Military and Intelligence Operations

■ WILLIAM C. HANEBERG

Geology and topography have placed important constraints on military operations since the beginning of organized warfare. The movement of troops on foot, on horseback, or in motorized vehicles can be hindered by topography and soil conditions. Bedrock type and strength are important factors in the construction of fortifications, the availability of groundwater supplies can control the location of military installations, and mountainous terrain can offer cover to guerilla forces or small groups of operatives. The collection and analysis of geologic information relevant to military operations falls into the discipline of military geology, and military geologic information is often referred to as terrain intelligence.

Two people with knowledge of geology are reported to have participated in Napoleon's invasion of Egypt in 1798. The first military operation guided by terrain analysis, however, was the defeat of Napoleon's troops near the Katzback River in Silesia by the Prussian general von Blucher in 1813. In 1823, the United States Military Academy became one of the first institutions of higher learning to offer instruction in geology. Geologic and topographic considerations continued to play an important role in military operations throughout the nineteenth century, for example at the Battle of Gettysburg in 1863. Union soldiers occupied boulder covered terrain underlain by a hard igneous rock known as diabase, which provided protection from Confederate soldiers advancing unprotected through flat fields underlain by softer shale and sandstone. The first extensive use of geology in military operations was probably during the Russo-Japanese War (1904–1905), when the Russian Army used geologists to provide advice on the construction of fortifications. The use of geologic information became commonplace during World War I and World War II, and included the creation of a military geology branch within the United States Geological Survey. The United States Army Topographic Engineering Center and the National Imagery and Mapping Agency (NIMA) currently provide a variety of products and services directly related to terrain intelligence.

One of the principal concerns of military geologists is trafficability, or the ease with which a landscape can be

traversed by troops. An assessment of trafficability requires knowledge of soil types (which are in turn controlled by the underlying bedrock type); the physical, chemical, and biological soil forming processes at work in an area; and meteorological conditions. Arctic areas underlain by permafrost, for example, may be trafficable in winter but impassible in summer when the upper portion melts. Likewise, desert lakebeds known as playas may be trafficable when dry but impassible after a short rainstorm. Trafficability can in some cases be assessed using published topographic maps, geologic reports, and soil surveys. In other cases, reconnaissance forces can use specialized trafficability instrument kits to conduct soil tests and obtain detailed information along potential routes.

Satellite or aircraft-based remote sensing technology can provide the information for terrain analysis and trafficability studies in denied or otherwise inaccessible areas. For example, multispectral satellite imagery can be used to remotely map soil and rock types based on the spectral reflectance of minerals. High-resolution satellite imagery can also be used to visually interpret geologic and topographic conditions. The Shuttle Radar Topography Mission, flown in February 2000, used synthetic aperture radar to produce an elevation data set covering 80% of Earth's land surface. The elevation data can be used to create topographic maps or three dimensional images of inaccessible areas for use in terrain analysis, virtual reality based training, flight simulators, and other military applications.

Manual terrain analysis is time consuming and requires the expertise of a trained specialist. The result is typically a map on which terrain is classified into three categories based upon trafficability: go, slow-go, and no-go. Current research is aimed at the creation of computer expert systems that will be able to combine map layers showing roads, soil types, topography, rivers, vegetation, and land use to produce probabilistic estimates of trafficability for specific vehicle types and weather conditions. These results will include estimates of the reliability of calculated trafficability values.

Geology also plays an important role in the survivability or penetrability of fortifications and facilities, particularly those constructed underground. Information about geology, particularly the strength of different rock types, is used in the design of underground structures that must resist conventional attack. Likewise, information about the geologic setting of an enemy facility can be used to select weapons and methods of attack that are most likely to be successful.

#### ■ FURTHER READING:

##### BOOKS:

Underwood, James R., Jr. and Peter L. Guth. *Military Geology in War and Peace*. Boulder, CO: Geological Society of America, 1998.

Zen, E-An and A.S. Walker. *Rocks and War: Geology and the Civil War Campaign of Second Manassas*. Shippensburg, PA: White Mane Publishing, 2000.

##### ELECTRONIC:

Leith, William. "Military Geology in a Changing World." *Geotimes*. February, 2002. <[http://www.agiweb.org/geotimes/feb02/feature\\_military.html](http://www.agiweb.org/geotimes/feb02/feature_military.html)> (11 February 2003).

Surdu, J.R., C. Gates, J. Sullivan, M. Rudak, N. Colvin, and K. Slocum. "Trafficability Analysis Engine." 23rd Army Science Conference. December 2-5, 2002. <<http://www.asc2002.com/summaries/e/EP-17.pdf>> (11 February 2003).

U.S. Army Corps of Engineers Topographic Engineering Center. "TEC Web Site." 2002. <<http://www.tec.army.mil/>> (11 February 2003).

##### SEE ALSO

*Geospatial Imagery*

*GPS*

*Mapping Technology*

*Natural Resources and National Security*

*NIMA (National Imagery and Mapping Agency)*

*Photography, High-Altitude*

*RADAR, Synthetic Aperture*

*Remote Sensing*

---

## Geospatial Imagery

---

■ WILLIAM C. HANEBERG

Geospatial imagery encompasses a wide range of graphical products that convey information about natural phenomena and human activities occurring on Earth's surface. The term can include color and panchromatic (black and white) aerial photographs, multispectral or hyperspectral digital imagery (including portions of the electromagnetic spectrum that lie beyond the range of human vision), and products such as shaded relief maps or three-dimensional images produced from digital elevation models. A related term, geospatial intelligence, describes the use of geospatial imagery for intelligence, security, or defense purposes.

The earliest form of geospatial imagery was aerial photography, which consists of photographs taken from an airborne or spaceborne camera. Aerial photographs can be taken either vertically, which is preferred if the photographs are to be used to prepare maps of an area, or obliquely. Overlapping vertical aerial photographs can be viewed stereoscopically to obtain a three-dimensional effect that can be useful for topographic or geologic analysis, and also used to create topographic maps. Another common form of geospatial imagery is the multispectral

or hyperspectral image, which can resemble a color photograph. Instead of being created by the interaction of visible spectrum light with chemicals, however, modern multispectral and hyperspectral images are created by measuring the response of an electronic sensor to a particular portion, or band, or the electromagnetic spectrum. The bands sampled by a sensor can extend far beyond the portion of the spectrum visible to the human eye; hence multispectral and hyperspectral imagery has the potential to convey much more information than a traditional photograph. Whereas multispectral images may consist of several bands, (perhaps representing infrared, red, green, and blue light), hyperspectral images can include information from more than 200 bands. Multispectral and hyperspectral bands that fall outside the range of human vision must be assigned colors if they are to be seen by humans. The resulting images are known as false color images because their chosen colors represent the intensity of the sensor response to invisible wavelengths, not wavelengths corresponding to the colors on the printed image. Synthetic aperture radar (SAR) images consist of information obtained by instrument that actively emits a radio signal rather than passively sensing naturally reflected radiation. SAR technology can be used to generate detailed topographic maps of Earth's surface from space, even in areas covered by clouds.

The resolution of geospatial imagery has increased over time. Keyhole intelligence satellites, which have been launched by the United States since the early 1960s, currently have a resolution on the order of 2 cm (although no images of this resolution have been released to the public). The resolution of geospatial imagery currently available to the public is far less than that of classified intelligence imagery. The Landsat 1 satellite, launched in 1972, had a resolution of 80 m. Landsat 7, launched in 1999, has resolutions of 15 m for panchromatic images, 30 m for six multispectral bands, and 60 m for its thermal band. The French SPOT 5 satellite obtains images ranging in resolution from 5 m for panchromatic to 20 m for infrared. The commercial Quickbird satellite, which was launched in 2001, provides commercially available imagery with 61 cm panchromatic and 2.44 m multispectral resolution. The commercial IKONOS satellite, launched in 1999, can produce 1 m resolution color images.

Within the United States, the National Imagery and Mapping Agency (NIMA) is the single agency that the federal government relies upon to manage the acquisition, interpretation, and dissemination of geospatial information and imagery. Although it is primarily a combat support agency within the Department of Defense, NIMA also provides support to federal policy makers and government agencies. NIMA was formed in 1996 by consolidating the Defense Mapping Agency, the Central Imagery Office, the Defense Dissemination Program Office, the National Photographic Interpretation Center along with some parts of the Defense Intelligence Agency, the National Reconnaissance Office, the Defense Airborne Reconnaissance Office, and the Central Intelligence Agency.

The collection and application of geospatial imagery in support of defense and intelligence operations is heavily dependent upon computer technology. Image processing software can be used to identify features on multispectral images according to their spectral signatures. The response of a multispectral sensor to grass or trees, for example, will be different than its response to a concrete road or steel building. Other applications include the use of sharpening filters to enhance images. Geographic information system (GIS) software can be used to combine different types of imagery, for example by superimposing a multispectral image and road network map on a shaded topographic relief map.

## ■ FURTHER READING:

### BOOKS:

- Bossler, John D., John R. Jensen, Chris McMaster, and Chris Rizo (editors). *Manual of Geospatial Science and Technology*. Mount Laurel, NJ: Taylor & Francis, 2001.
- Campbell, James B. *Introduction to Remote Sensing*, 3rd edition. New York: Guilford Press, 2002.
- U.S. Department of Defense. *21st Century Complete Guide to the National Imagery and Mapping Agency (NIMA): Geospatial Intelligence for National Security, Geodesy for the Layman, Combat Support, Terrain Visualization*. Mount Laurel, NJ: Progressive Management, 2003.

### ELECTRONIC:

- International Society for Photogrammetry and Remote Sensing, c/o Ian Dowman, Department of Geomatic Engineering, University College London, Gower Street, London WC1E 6BT, United Kingdom. <<http://www.isprs.org/>>.
- National Imagery and Mapping Agency. "NIMA HOME." <<http://www.nima.mil/>> (7 March 2003).
- Short, Nicholas M., Sr. "The Remote Sensing Tutorial." NASA. October 22, 2002. <<http://rst.gsfc.nasa.gov/>> (7 March 2003).
- Skorve, Johnny E. "Using Satellite Imagery to Map Military Bases of the Former Soviet Union." *Earth Observation Magazine*. April 2002. <<http://www.eomonline.com/Common/currentissues/Apr02/skorve.htm>> (7 March 2003).
- U.S. Geological Survey "Ask USGS: Satellite Imagery." August 19, 2002. <<http://ask.usgs.gov/satimage.html>> (7 March 2003).

### SEE ALSO

*Bomb Damage, Forensic Assessment Cameras*  
*Cuban Missile Crisis*  
*Electromagnetic Spectrum*  
*Electro-Optical Intelligence*  
*Geospatial Imagery*  
*LIDAR (Light Detection and Ranging)*  
*Photographic Resolution*  
*Photography, High-Altitude*  
*RADAR, Synthetic Aperture*  
*Remote Sensing*  
*U-2 Spy Plane*  
*Unmanned Aerial Vehicles (UAVs)*

## Germany, Counter-Terrorism Policy

■ JUDSON KNIGHT

Since the 1972 Olympics in Munich, counter-terrorism—the use of military, law enforcement, intelligence, and other resources to identify, circumvent, and neutralize terrorist groups within a country—has been among the principal security concerns in Germany. This priority has changed little with the reunification of the country in 1990; rather, the states of eastern Germany have been integrated into the federal system, which provides the framework for response to terrorist threats.

### The Lessons of 1972

When the West German city of Munich hosted the Olympic Games in 1972, it was the first time in 36 years that Germany had hosted the Olympic Games. Whereas Hitler had used the 1936 Olympics as a showcase for Nazi power, the West Germans of 1972 were eager to show that theirs was an open, peaceful, and democratic society. For that reason, the Germans took few measures to protect the athletes at the Olympic Village in Munich. Nor did it seem, in 1972, that such measures were necessary; at that time, the world had little exposure to modern terrorism, with its hijacking, hostage-taking, and other acts of crime under cover of political action.

All of that would change on September 5, 1972, when eight Palestinian terrorists entered an apartment building that housed the Israeli delegation to the Olympics. By the time the day was over, after more than 18 hours in which police surrounded the Olympic Village and the terrorists negotiated with authorities, nine Israeli athletes and one German policeman lay dead. In the aftermath of the Olympic terror, security became a priority not only for the Olympic Games, whose athletes' compounds were heavily secured thereafter, but for nations facing the threat of terrorism. German counter-terrorist policy thus emerged from the painful lessons of Munich.

### The German Counter-Terrorist Structure

Directing counter-terrorism in Germany is the coordinator for Intelligence, or *Koordinierung der Nachrichtendienste des Bundes*, who has the ear of the chancellor—the nation's head of government—and who coordinates state efforts under a general national policy. Actual day-to-day implementation of counter-terrorist activities is the work of the Federal Ministry of the Interior, under whose auspices are police, intelligence agencies, and border police. In line with the federal model on which the German political

system is built, each state has its own ministry of the interior, which also has police, intelligence, and emergency preparedness responsibilities for local situations.

Many aspects of the German counter-terrorism structure are similar to those of France. However, the French—despite their heavily centralized government—permit a regional political appointee, or *préfet*, to assume control in the event of a local incident. The *préfet* oversees police and emergency activities on the scene. By contrast, in Germany the federal police, when directed to do so by the federal prosecutor or state authorities, take control in terrorist situations. They are usually assisted by state police, which are likely to be the first responders in the event of a local incident.

The Federal Criminal Police (*Bundeskriminalamt*), an office of the Ministry of the Interior, provides protection for dignitaries, and investigate acts of terrorism. Intelligence is gathered by a number of agencies, including the German Intelligence Service, or *Bundesnachrichtendienst*. Within the states, the State Criminal Police (*Ländeskriminalamt*) conduct criminal investigations.

**BGS and GSG 9.** The Federal Border Guard (BGS or *Bundesgrenzschutz*), although they act in a federal capacity, are directed by the states' ministries of the interior. It is the responsibility of the BGS to secure borders, transportation sites, and other sensitive federally controlled areas. Within the BGS is an elite counter-terrorist organization, analogous to the U.S. Delta Force, the British SAS, or the French GIGN. This is GSG 9, or *Grenzschutzgruppe 9*. A direct outgrowth of the Munich massacre, GSG has taken part in over 1,300 operations since its inception. One of the most notable of these—and one of only a handful of times when GSG 9 has been required to use firearms—was the rescue of passengers aboard a Lufthansa flight hijacked by Arab terrorists in October 1977.

The terrorists, who were working with Germany's notorious Red Army Faction (sometimes known as the Baader Meinhof Gang), seized control of the plane on its way from the Balearic Islands to Germany. Denied landing in a number of locations, the plane finally made its way to Mogadishu, Somalia. There, after Somali troops distracted the hijackers by lighting a bonfire in front of the aircraft, two GSG 9 groups, assisted by SAS personnel, stormed the plane. All of the more than 80 passengers survived, and all but one of the terrorists died in the assault.

#### ■ FURTHER READING:

##### BOOKS:

*Combatting Terrorism: How Five Foreign Countries Are Organized to Combat Terrorism.* Washington, D.C.: General Accounting Office, 2000.

Linde, Erik J. G. van de. *Quick Scan of Post 9/11 National Counter-terrorism Policymaking and Implementation in Selected European Countries: Research Project for the*

*Netherlands Ministry of Justice*. Santa Monica, CA: RAND Europe, 2002.

Tophoven, Rolf. *GSG 9, German Response to Terrorism*. Koblenz, Germany: Bernard & Graefe Verlag, 1984.

#### PERIODICALS:

Hoffman, Bruce. "Is Europe Soft on Terrorism?" *Foreign Policy* no. 115 (summer 1999): 62–76.

#### ELECTRONIC:

Calahan, Alexander B. "Countering Terrorism: The Israeli Response to the 1972 Munich Olympic Massacre and the Development of Independent Cover Action Teams." Federation of American Scientists. <<http://www.fas.org/irp/eprint/calahan.htm>> (February 22, 2003).

#### SEE ALSO

*European Union*  
*France, Counter-Terrorism Policy*  
*Germany, Intelligence and Security*

---

## Germany, Intelligence and Security

---

Germany is an active, key participant in the North Atlantic Treaty Organization (NATO) and the European Union (EU), working closely with neighboring European nations and the United States on international economic, intelligence, and security issues. However, Germany weathered a turbulent and sometimes violent past century. Germany is currently one of the world's leading democratic governments, but for the nation's intelligence and security agencies, overcoming the legacy of their role in two world wars, the Nazi government, the Holocaust, and Soviet-dominated East Germany, has proved a formidable challenge.

During the late nineteenth century and through World War I, the German *Abwehr* was one of the world's leading, most sophisticated, and successful intelligence agencies. The *Abwehr* maintained one of the largest spy networks and made tremendous advances in the technology of espionage, cryptology, and signals intelligence. During World War II, the *Abwehr* was again successful in many operations, especially in the recruitment of double agents who infiltrated Allied military installations. Some of the *Abwehr*'s leading officers opposed Nazi rule, and organized a failed attempt to assassinate Nazi leader Adolf Hitler. The organization was dissolved before the fall of the Third Reich.

While the *Abwehr* was operated much like any other modern intelligence agency, some German intelligence agencies of the era were more sinister. In 1941, Hitler issued a directive known as the "Night and Fog Decree." This decree elevated Nazi intelligence and security agencies such as the *Gestapo* above the law, granting them

sweeping powers of arrest, detainment, torture, and imprisonment of persons suspected of anti-government offenses. The decree was expanded to cover the arrest, detainment, and deportation to concentration camps of Jews, gypsies, prisoners of war, and political dissidents.

After the war, Germany was partitioned into two separate nations. Soviet influenced East Germany employed a powerful secret police and intelligence force, known as the STASI. The East German government charged the STASI with spying on citizens to ferret-out political dissidents. The force gained an oppressive and brutal reputation much like that of its Nazi predecessors. In 1989, the fall of Communist East Germany and the Berlin Wall began Germany's reunification process. After endeavoring for decades to heal the wounds of Nazism, the German government had to address the oppressive legacy of former East German government agencies. After the formal reunification of Germany, government leaders set forth a highly publicized campaign to restructure and reform the re-emergent nation's intelligence and security agencies. Today's German intelligence community has actively sought to distance itself from its predecessors.

Germany's primary intelligence agency is the *Bundesnachrichtendienst* (BND), the Federal Intelligence Service. The BND handles both internal and external intelligence and is part of the Federal Chancellor's Office, the German government's executive office. The BND manages a substantial network of human intelligence worldwide and conducts extensive radio and signals surveillance in Germany and throughout Europe. Working in cooperation with other security agencies, especially the Federal Criminal Police, the BND collects information relevant to the location and prosecution of terrorist groups, illegal narcotics traffickers, money launderers, and arms dealers. In accordance with international law, the BND conducts intelligence operations aimed at preventing the proliferation of nuclear technology and materials.

Aside from the BND, the German intelligence community makes the traditional distinction between internal and external intelligence and divides their military and civilian intelligence agencies accordingly. Military intelligence is coordinated by individual branches of the armed forces and the Defense Ministry. The primary military intelligence agency is the *Amt für Nachrichtenwesen der Bundeswehr* (ANBw), or the Office of Federal Armed Forces Intelligence. ANBw coordinates the operations of various branches of military intelligence and facilitates the sharing of vital intelligence information with civilian agencies in the German intelligence community. ANBw primarily assesses the military strength, operations, and political position of foreign militaries.

The *Militärischer Abschirmdienst* (MAD), Military Security Service, is responsible for counterintelligence operations. One of the federal intelligence offices, MAD collects intelligence on foreign intelligence operations, and assesses security systems intended to guard classified materials and maintain military secrecy when needed. MAD advises the armed forces and German government



on security issues. The counterintelligence agency relies on the cooperative efforts of the *Amt für Fernmeldwesen Bundeswehr* (AFMBw), the Office for Radio Monitoring of the Federal Armed Forces, when conducting surveillance operations.

The Interior Ministry administers Germany's civilian intelligence agencies. Charged with collecting and analyzing internal intelligence and security information, the nation's main civilian agencies are the *Bundesamt für Sicherheit in der Informationstechnik* (BSI), Federal Office for Information Technology Security, and the *Bundesamt für Verfassungsschutz* (BfV), Federal Office for the Protection of the Constitution. The BSI is responsible for the security of all government information technology. The office assesses potential security threats, and develops protective measures to guard sensitive and classified materials. While mainly concerned with government information systems, the BSI has also conducted operations to assess the security of the nation's banking computer systems. The office publishes a yearly manual on information technology security, and distributes it to German corporations. The BSI also conducts surveillance of Internet and information systems crimes, such as fraud.

The Federal Office for the Protection of the Constitution (BfV) assesses risks posed by various extremist groups. The agency conducts surveillance operations and infiltrates extremist groups to gather information about their organization, financial resources, weapons, and plans for action. The BfV is not a censorship organization, and does not conduct espionage against law-abiding citizens. The BfV's mission is to monitor extremists and paramilitary groups that pose a potential threat to national interests. Extensive intelligence resources are devoted to monitoring and destroying Neo-Nazi groups that are banned under German law.

In its most important capacity, the BfV interprets and processes all information regarding espionage cases. When necessary, the agency shares this information with Federal Police, justice officials, and defense lawyers.

Germany participates in many international intelligence operations, including global anti-terrorism measures. In recent years, the German intelligence community has become one of the main sources of information on extremist political organizations and subversive groups throughout Europe.

#### BOOKS:

- Browder, George C. *Hitler's Enforcers: The Gestapo and SS Security Service in the Nazi Revolution*. Oxford: Oxford University Press, 1996.
- Childs, David and Richard Popplewell. *The Stasi: The East German Intelligence and Security Service*. New York: New York University Press, 1996.
- Schiel, Katy. *Inside Germany's BND: The Federal Intelligence Service (Inside the World's Most Famous Intelligence Agencies)*. New York: Rosen Publishing Group, 2003.

#### SEE ALSO

*European Union  
Germany, Counter-Terrorism Policy*

---

## Gestapo

---

■ ADRIENNE WILMOTH LERNER

The *Geheime Staatspolizei*, or Gestapo, a German secret police force, was created in 1933 after Adolf Hitler became chancellor of Germany. The Gestapo was created to help solidify Nazi control by identifying and arresting anti-Nazi agents in Germany. The agency was restructured several times during its twelve year history and was instrumental in perpetrating the Nazi deportation and destruction of European Jews during the Holocaust.

Hitler named Herman Göring the director of the Gestapo soon after its founding. Göring encouraged his officers to root out and arrest leftist sympathizers, especially communists, whom he considered a threat to the Nazi government. He also oversaw the Gestapo's enforcement of the anti-Semitic Nuremberg Laws. In 1936, Heinrich Himmler, head of Hitler's special forces unit, the *Schutzstaffel* (SS), was given command of the Gestapo and the *Kriminalpolizei*, or Kripo.

In 1939, in the months prior to the beginning of the second world war, Hitler reorganized the German armies. The Gestapo was integrated, with the rest of the Nazi police and intelligence organizations, into the *Reichssicherheitshauptamt* (RHSa) under the direction of Reinhard Heydrich. Though officially part of the Reich Security Central Office, the organization remained popularly known as the Gestapo.

At the outbreak of the Second World War in 1939, there were approximately 40,000 Gestapo agents in Germany. As the war progressed and the Nazis gained territory throughout Europe, the Gestapo swelled to employ over 150,000 informants, agents, and accessory personnel. Gestapo agents were charged with rooting out foreign agents and resistance fighters, but they also expanded their role as an internal police force. Gestapo agents and informants concentrated on finding suspected political dissidents of the Third Reich. Spying on citizens became pervasive, and the Gestapo encouraged people to turn in "suspect persons" to local authorities. While victims of the Gestapo were subject to both civil and criminal prosecution, the secret police themselves operated above the law. On February 10, 1936, the Nazi government officially decreed that the organization was not subject to judicial review. There were no legal restraints on detention of suspects, evidence collection, or police violence. This lack of legal restraint, paired with the Gestapo's tendency to attract and employ Nazi extremists and former criminals



Heinrich Himmler, chief of the Gestapo, the German secret police, poses in his military uniform in 1938. AP/WIDE WORLD PHOTOS.

in its ranks, permitted the brutality for which the force became infamous.

The Gestapo also aided intelligence work during the war, but the department was secondary to the *Sicherheitsdienst* (SD), or Security Service. The department employed counter-intelligence agents, ciphers, and oversaw a vast network of informants in Allied countries. In the occupied territories, the Gestapo infiltrated partisan resistance groups. The organization also aided the massive Nazi propaganda campaign both before and during the war.

Intelligence, security, and police forces often overlapped in jurisdiction during the Nazi regime. Several departments performed the same functions, and were often in conflict with each other. The Abwehr, the intelligence service under the direction of spymaster Wilhelm Canaris, negotiated an agreement with the SD about their respective roles. Despite the agreement, both organizations maintained their own network of spies and informants, and did not often coordinate their international operations. In 1943, Canaris and several other key members of the Abwehr joined the Resistance movement against the Nazi government. Canaris used the Abwehr intelligence network to leak secrets and troop positions to the Allies. The Gestapo investigated Canaris and the Abwehr, and in 1944, after a failed attempt to assassinate Nazi

leader Adolf Hitler, liquidated the Abwehr intelligence service. Canaris and his followers were executed. The discovery of the July Plot to assassinate Hitler, and Canaris' spy ring was a key counter-intelligence victory for the Gestapo, SD, and RHSA.

The Gestapo, as well as its parent organization, the SS, aided the *Einsatzgruppen*, or mobile killing units, responsible for the massacre of nearly one million Jews during the Holocaust. Gestapo and SS members also tracked down refugees in hiding and policed ghettos and concentration camps. After the war at the Nuremberg trials of Nazi war criminals, the Gestapo was named as one of the chief institutional perpetrators of the Holocaust.

The Gestapo was dissolved with the fall of the Third Reich in 1945.

#### ■ FURTHER READING:

##### BOOKS:

Browder, George C. *Hitler's Enforcers: The Gestapo and SS Security Service in the Nazi Revolution*. Oxford: Oxford University Press, 1996.

Gellately, Robert. *The Gestapo and German Society*. Oxford: Oxford University Press, 1991.

##### SEE ALSO

*French Underground during World War II, Communication and Codes*

*Germany, Intelligence and Security World War II*

## GIS

#### ■ K. LEE LERNER

GIS is the common abbreviation for Geographic Information Systems, a powerful and widely used computer database and software program that allows scientists to link geographically referenced information related to any number of variables to a map of a geographical area. GIS allows its users to analyze and display data using digitized maps. In addition, GIS can generate maps and tables useful to a wide-range of applications involving planning and decision-making. GIS programs allow the rapid storage, manipulation, and correlation of geographically referenced data (i.e., data tied to a particular point or latitude and longitude intersection on a map).

In addition to scientific studies, by 2003, GIS programs were in wide use in a number of emergency support agencies and systems (e.g., the Federal Emergency Management Agency (FEMA)).



Members of the investigating team inspect part of the left wing from the Space Shuttle *Columbia* wreckage in the hangar where it is reconstructed at the Kennedy Space Center in Cape Canaveral, Florida. NASA engineers used GIS mapping technology to map debris field patterns that helped narrow the areas to be searched. AP/WIDE WORLD PHOTOS.

GIS programs allow scientists to layer information so that different combinations of data plots can be assigned to the same defined area. GIS also allows users to manipulate data plots to predict changes or to interpret the evolution of historical data.

GIS maps are able to convey the same information as conventional maps, including the locations of rivers, roads, topographical features, and geopolitical information (e.g., location of cities, political boundaries, etc.). In addition, to conventional map features, GIS offers geologists, geographers, and other scholars the opportunity to selectively overlay data tied to geographic position. By overlaying different sets of data, scientists can look for points or patterns of correspondence. For example, rainfall data can be layered over another data layer describing terrain features. Over these layers, another layer data representing soil contamination data might be used to identify sources of pollution. In many cases, the identification of data correspondence spurs additional study for potential causal relationships.

GIS software data plots (e.g., sets of data describing roads, elevations, stream beds, etc.) are arranged in layers that can be selectively turned on or turned off.

NASA engineers and teams of other scientists—including researchers and undergraduates from Stephen F. Austin University in Nacogdoches, Texas—employed GIS mapping to map remains found after the break up of the space shuttle *Columbia* in January 2003. Debris field maps helped narrow search patterns and—by linking the location of debris—allowed engineers and investigators to reconstruct critical elements of the disaster sequence. GPS data were used to construct the debris maps and to provide accurate representations of the retrogressive pattern of debris impacts.

GIS technology can also aid epidemiologists in tracking diseases and would be instrumental in the early identification of patterns of disease that could reveal a bioterrorist attack.

#### ■ FURTHER READING:

##### BOOKS:

- Rigaux, P. et al. *Spatial Databases: With Application to GIS*. Morgan Kaufmann, 2001.
- Steede-Terry, K. *Integrating GIS and the Global Positioning System*. ESRI Press, 2000.

## SEE ALSO

*Forensic Geology in Military or Intelligence Operations*  
*Geologic and Topographical Influences on Military and Intelligence Operations*  
*Geospatial Imagery*

## Global Communications, United States Office

President George W. Bush created the Office of Global Communication (OGC) through executive order in January, 2003. The OGC, a White House office, is headed by the deputy assistant to the president for Global Communications. The OGC's mission is to shape and disseminate news and information about the United States in areas of the world with high anti-American sentiments.

In the aftermath of the September 11, 2001 terrorist attacks on the World Trade Center and the Pentagon, American observers noted that anti-American sentiment was widespread in the Middle East, Southeast Asia, North Africa, and other parts of the world. The Bush administration established the OGC to decrease the fervor and prevalence of these sentiments by thoroughly and clearly explaining the foreign policy and values of the United States. The OGC not only endeavors to explain the positions of the United States, it will also seek to actively encourage open dialogue between the United States and its detractors. The Bush White House established the OGC to provide a united voice for spreading America's message.

The OGC replaced and expanded the operations of the Coalition Information Center (CIC), which distributed information to the press in Afghanistan during Operation Enduring Freedom. Unlike the CIC, the OGC focuses on more than military operations. In many respects, the OGC is an office to market all facets of American policies and life to the world. The OGC's does not focus solely on countries that have a negative image of the United States. The Bush administration also uses the OGC to coordinate the formulation and dissemination of positive information on U.S. foreign policy to American allies in Europe.

The OGC accomplishes its objectives through several means, including sending out daily talking points to reporters around the world. The OGC also arranges interviews for American representatives on foreign language television networks. In 2003, before and during the war in Iraq, the OGC placed American officials including Secretary of Defense Donald Rumsfeld on Al-Jazeera and other Arabic language networks to advocate America's stance against Iraq.

Critics argue that the OGC's spin is not well received in parts of the world already hostile to the United States. The Bush administration, however, argues that the OGC

will continue to play an important role in the administration's efforts to reduce anti-American sentiment, even though such a project may take years to produce substantial results.

### ■ FURTHER READING:

#### ELECTRONIC:

United States Office of Global Communications. <<http://www.whitehouse.gov/ogs>> (May 9, 2003).

## *Glomar Explorer*

### ■ ADRIENNE WILMOTH LERNER

The Hughes *Glomar Explorer* was a salvage ship built for a clandestine Central Intelligence Agency mission to retrieve a sunken Soviet submarine. The United States government approached billionaire Howard Hughes in the late 1960s with a proposal to build the vessel under the guise of a business venture to mine manganese nodules off the ocean floor. The building of *Glomar Explorer*, or Hughes Mining Barge 1, and the submarine recovery effort were code named Project Jennifer.

On April 11, 1968, Naval Intelligence at Pearl Harbor intercepted distress messages from a Soviet submarine. The submarine, located in waters approximately 750 miles northwest of Hawaii, reported an onboard explosion while near the surface and then quickly sank. Hoping to find the wreckage of the submarine and recover the ballistic missiles on board, the Soviet fleet launched a search party. After two months of searching, the Soviets failed to locate their downed ship.

The Golf-class diesel submarine was one of the older vessels in the Soviet fleet, but nonetheless, the prospect of retrieving Soviet technology, nuclear weapons, and codebooks was enticing to American intelligence agencies. Because it could not send marked American Naval vessels to recover the sunken submarine without arousing suspicion from the Soviets, Naval intelligence enlisted the help of billionaire Howard Hughes to construct the specialized equipment and ship necessary for the salvage project. The six-year venture to build the ship and raise the Soviet submarine operated under the guise of a deep-sea mining operation.

Recovery efforts began on June 20, 1974. The 63,000-ton *Glomar Explorer* located the wreckage on the seabed at a depth of 17,000 feet (5,200 m) and scouted the downed vessel. *Glomar Explorer* had been fitted with a giant claw mechanism, nicknamed Clementine. A series of tethers stabilized the claw during underwater maneuvers. As the salvage effort began, the *Glomar Explorer* crew lowered Clementine to the wreck site. When the claw was nearly into position, an operator error at the controls sent the



The Hughes *Glomar Explorer*, a 618-foot-long ship used in the partial recovery of a sunken Soviet submarine in the Pacific Ocean, northwest of Hawaii. AP/WIDE WORLD PHOTOS.

claw careening into the sea floor. The salvage effort continued, however, and the claw was positioned around the ship. When the wreckage of the Soviet submarine was about a mile (1.6 k) from the water's surface, three of the mechanical claw's tines malfunctioned, apparently damaged in the crash into the ocean floor. Unable to sustain its own weight, the wrecked Soviet submarine tore apart. The crew aboard *Glomar Explorer* tensely waited for the broken part of the wreckage to hit the sea floor, fearing detonation of weapons on board the submarine.

While the crew of *Glomar Explorer* remained safe, the salvage effort suffered a substantial loss. Only the forward section of the ship was ultimately recovered. The CIA recovered Soviet communications apparatus, a few ballistic missiles, and various codebooks. A majority of the desired items and information, including most of the nuclear weapons and the Soviet crypto keys, remained on the sea floor in the wreckage.

The remains of six Soviet sailors were found in the recovered section of the submarine. The crew of the *Glomar Explorer* gave the sailors a ceremonial burial at sea, conducted in Russian.

In 1975, reporters from the *Los Angeles Times* broke the story of the *Glomar Explorer*. In the following months,

various articles linked the *Glomar Explorer*, and its cover as deep-sea mining operation, to the CIA and the submarine salvage effort. After reporters appealed to the government for information on Project Jennifer, CIA officials refused to acknowledge the existence of any records pertaining to the operation. Since then, the terms "Glomar response" and "Glomarization" have been applied to situations when the existence of government documents is neither confirmed nor denied. Most of the records concerning Project Jennifer were declassified in 1995.

Although the submarine salvage effort did not meet expectations, and the *Glomar Explorer* was retired to dry dock for over fifteen years, the ship was completely overhauled in 1996 and converted for use in commercial exploration and deep-sea drilling.

#### ■ FURTHER READING:

##### BOOKS:

Burleson, Clyde W. *The Jennifer Project*. College Station: Texas A&M University Press, 1997.

Varner, Roy D. *Matter of Risk: The Incredible Inside Story of the CIA's Hughes Glomar Explorer Mission to Raise a Russian Submarine*. New York: Random House, 1979.

## Government Ethics (USOGE), United States Office

The United States Office of Government Ethics (OGE) is charged with setting standards intended to regulate and ensure ethical conduct of personnel within the executive branch. The office's mission is to prevent personnel from using their position in the federal government for personal gain (monetary or otherwise), and to prevent fraud and abuses of power. Acting as an impartial review committee, the OGE also assesses cases of conflict of interest and ensures the veracity of financial and personal information provided by executive branch officials. The overall purpose of the OGE is to maintain a high standard of ethics in the practice of government and to build and maintain public trust.

The OGE is an independent agency within the executive branch. The director of the office, who is appointed by the president, oversees four divisions, each of which is responsible for different duties. The office of the director is charged with the verification and analysis of personal financial records of high-level members of the executive branch for conflicts of interest and violations of campaign finance, donation, and personal gain regulations. The director of the OGE also certifies similar disclosures for presidential appointments before sending the records to Senate for discussion of confirmation.

The Office of General Counsel and Legal Policy maintains the policy and legal structure of ethical practice and review in the executive branch. The committee advises necessary offices of changes laws and regulations, and recommends new policy to strengthen existing programs. General Counsel is also responsible for media relations for the OGE.

The Office of Government Relations and Special Projects (OGRSP) is responsible for advising Congress, the Office of Management and Budget, and the president on ethical implications of monetary, economic, and corporate policy. In recent years, the committee has addressed, in the wake of the Enron scandal, domestic corporate fraud and international anti-corruption measures.

The Office of Agency Programs (OAP) manages personnel education programs on ethics issues. The office coordinates ethics regulations and enforcement of ethical conduct with ethical review boards in the individual agencies of the executive branch.

### ■ FURTHER READING:

#### ELECTRONIC:

United States Department of Government Ethics. <<http://www.usoge.gov>>(December 1, 2002).

## GPS

Global Positioning System (GPS) is a navigation system consisting of a constellation of 24 navigational satellites orbiting Earth, launched and maintained by the U.S. military. GPS satellites orbit at approximately 11,000 mi (17,700 km) above Earth, with orbit periods of approximately 10 hours. The final satellite was placed in orbit in 1993. Because each satellite houses cesium and rubidium atomic clocks that are periodically updated and synchronized with a ground station in Colorado, GPS receivers can decode signals from the satellites to calculate location and exact time.

To overcome shortcomings in earlier navigation systems, United States developed another system: Navstar (Navigation Satellite for Time and Ranging) Global Positioning System. This system consists of 24 operational satellites equally divided into six different orbital planes (each containing four satellites) spaced at 60° intervals. The new system can measure to within 33 ft, (10 m), whereas earlier systems (e.g. Transit) were accurate only to 0.1 mi (0.16 km). Military users have access to systems with still greater accuracy.

Ground users commonly rely on GPS receivers. The receivers are small, hand-held devices that receive and decode GPS satellite signals. Small differences in the time lapse between signal receptions from three orbiting satellite signals (allowing triangulation of signals) are mathematically converted to latitude, longitude, and altitude. Sophisticated hand-held units are capable of determining latitude and longitude to a thousandth of an arc minute; these units show changes in reading as vehicles move very short distances).

With GPS, two types of systems are available with different frequencies and levels of accuracy. The Standard Positioning System (SPS) is used primarily by civilians and commercial agencies. As of midnight, May 1, 2000, the SPS system became 30 times more accurate when President William Jefferson Clinton ordered that the Selective Availability (SA) component of SPS be discontinued. SA was the deliberate decrease of accurate positioning information available for commercial or civilian use. The SPS obtains information from a frequency labeled GPS L1. The United States military has access to GPS L1 and a second frequency, L2. The use of L1 and L2 permits the transfer of data with a higher level of security. In addition to heightened security, the United States military also has access to much more accurate positioning by using the Precise Positioning System (PPS). Use of the PPS is usually limited to the U.S. military and other domestic government agencies.

Long before the space age, people used the heavens for navigation. Besides relying on the sun, moon, and stars, the early travelers invented the magnetic compass, the sextant, and the seagoing chronometer. Eventually,



A United States Customs official, right, receives instruction on LoJack, a technology that utilizes GPS, intended to help recover stolen cars before they are smuggled out of the United States. AP/WIDE WORLD PHOTOS.

radio navigation in which a position could be determined by receiving radio signals broadcast from multiple transmitters came into existence. Improved high frequency signals gave greater accuracy of position, but were sometimes blocked by high terrain and could not bend over the horizon. This limitation was overcome by moving the transmitters into space on Earth-orbiting satellites, where high frequency signals could accurately cover wide areas.

The principle of early satellite navigation was relatively simple. When a transmitter moves toward an observer, the Doppler shifted radio waves have a higher frequency, just like a train's horn sounds higher as it approaches a listener. A transmitter's signal will have a lower frequency when it moves away from an observer. If measurements of the amount of shift in frequency of a satellite radiating a fixed frequency signal with an accurately known orbit are carefully made, the observer can determine a correct position on Earth.

The United States Navy developed such a system, named Transit, in the late 1960s and early 1970s. Transit

helped submarines update their on-board inertial navigation systems. After nearly ten years of perfecting the system, the Navy released it for civilian use. However, a major drawback to Transit was that it was not accurate enough; a user had to wait until the satellite passed overhead, position fixes required some time to be determined, and an accurate fix was difficult to obtain on a moving platform.

Both Transit and Navstar use instantaneous satellite position data to help users traveling from one place to another. But another satellite system uses positioning data to report where users have been. This system, called Argos, is a little more complicated: an object on the ground sends a signal to a satellite, which then retransmits the signal to the ground. Argos can locate the object to within 0.5 mi (0.8 km). It is used primarily for environmental studies. Ships and buoys can collect and send data on weather, currents, winds, and waves. Land-based stations can send weather information, as well as information about hydrologic, volcanic, and seismic activity. Argos



A Brazilian federal police officer uses GPS technology in anti-drug operations near Brazil's border with Colombia in 2000. AP/WIDE WORLD PHOTOS.

can be used with balloons to study weather and the physical and chemical properties of the atmosphere. In addition, the system is being perfected to track animals, including marine life.

In addition to GPS use in weapons systems and for navigation, use of the GPS system in everyday life is becoming more frequent. Equipment providing and utilizing GPS is shrinking both in size and cost, while it increases in reliability. The number of people able to use the systems is also increasing. GPS devices are being installed in cars to provide directional, tracking, and emergency information. Emergency personnel can respond more quickly to 911 calls using tracking signal devices in their vehicles and in the cell phones of the person making the call. As technology continues to advance the accuracy of navigational satellite and without the impedence of Selective Availability, the uses for GPS will continue to develop.

#### ■ FURTHER READING:

##### BOOKS:

Balazs, G. H. "Homeward bound: satellite tracking of Hawaiian green turtles from nesting beaches to foraging pastures." *Proceedings of the Thirteenth Annual Symposium on Sea Turtle Biology and Conservation*. U.S. Dep.

Commer., NOAA Tech. Memo. NOAA-TM-NMFS-SEFSC-341, (1994):205–208.

El-Rabbany, Ahmed. *Introduction to GPS: The Global Positioning System* Norwood, MA: Artech Publishing, 2002.

##### ELECTRONIC:

Dana, Peter H. "Global Positioning Overview" The Geographer's Craft Project. May 1, 2000. University of Colorado. <[http://www.colorado.edu/geography/gcraft/notes/gps/gps\\_f.html](http://www.colorado.edu/geography/gcraft/notes/gps/gps_f.html)> (March 29, 2003).

##### SEE ALSO

*Mapping Technology*

## Great Game

#### ■ ERIC v.d. LUFT

In intelligence history, the "Great Game" described a complex rivalry—characterized by wars, assassinations, and espionage conspiracies—between Britain and Russia for control of Central Asia and the Near East.



In many critical facets, the mentality of the Great Game foreshadowed that of the Cold War and remains an important factor in world geopolitics at the dawn of the twenty-first century. The Soviet Union's incursion into Afghanistan in 1979 prompted the United States to support the Mujahedin throughout the 1980s. Ultimately, during the coursings of shifting political priorities, the United States formed and then broke ties with a number of factions—including Mujahedin elements that eventually found their way into the Taliban regime (deposed by the United States in 2002) and the al-Qaeda terrorist organization.

The deep suspicion and resentment that many of the Islamic peoples of Iran, Chechnya, Afghanistan, Pakistan, and neighboring regions now harbor against Russia, Britain, and more recently the United States, may in part be explained by the region's experience with—and resistance to—the imperialism of the Great Game.

**The "Tournament of Shadows."** The main friction points were the Black Sea, the Baltic regions, Persia, Afghanistan, Kashmir, the Punjab, and the steppes and deserts between the Caspian Sea and China. The Russians called this extended intrigue the "Tournament of Shadows," a term coined by Count Karl Robert Nesselrode (1780–1862), but in the West it was known as the "Great Game," apparently the coinage of Arthur Conolly (1807–1842), a British military diplomat and spy against Russia in Persia, the Caucasus, and the Himalayas from 1829 until Nasrullah Khan, emir of Bokhara (reigned 1826–1860), beheaded him in 1842.

In the mid-nineteenth century the two greatest world powers were Britain under Queen Victoria (1819–1901) and Russia under Czars Nicholas I (1796–1855), Alexander II (1818–1881), and Alexander III (1845–1894). This was true despite the acknowledged naval superiority of France over Russia. Russia was jealous of Britain's conquest of India and ascendancy over France since the end of the Napoleonic Wars. Russia was especially worried that British expansion along the northwest frontier of India would eventually threaten its own borders and thwart its longstanding quest for the warm-water port it needed to enhance both its navy and its merchant fleet.

From 1804 to 1864 the czars gained territory between the Black and Caspian Seas and from 1824 to 1895 they vigorously expanded west of the Caspian Sea into Kazakhstan, Turkmenistan, Uzbekistan, Kyrgyzstan, and Tajikistan, threatening China as well as the Ottoman Empire, Persia, Afghanistan, and India. This rapid and steady expansion of the Russian Empire into Central Asia alarmed the British, but there was little they could do about it. They soon began sending spies among native populations to learn of Russian intentions and to forge alliances against possible Russian incursions.

The earliest sortie of the Great Game was the expedition of Henry Eldred Pottinger (1789–1856) and Charles

Christie (d. 1812) from Bombay through Baluchistan to Herat in 1810. Their mission was to spy out possible overland routes by which Russia might invade India. Meanwhile John Malcolm (1769–1833) was negotiating with Persia to prevent any such attack. John Macdonald Kinneir (1782–1830) analyzed these routes and published his results in *A Geographical Memoir of the Persian Empire* (1813). Similar probes by both the Russians and British, such as the journey of Nikolai Nikolaevich Muraviev (1794?–1866) to Khiva in 1819 and that of William Moorcroft (1767–1825) to Bokhara in 1820, soon became common.

The exploits of General Alexis Yermolov (1772–1861), the Russo-Persian War (1827–1828), and the Russo-Turkish War (1828–1829) all further aroused British suspicion that Russia might have designs on India via Persia. Colonel George de Lacy Evans (1787–1870) galvanized these nascent fears with two pamphlets, *On the Designs of Russia* (1828) and *On the Practicability of an Invasion of India* (1829). British spies and military advisers actively helped Persian Prince Abbas Mirza (1783–1833) against Russia in the 1820s.

Evidence is strong, but proof remains absent, that Russian spies fomented unrest among the various native populations of the Indian subcontinent and surrounding lands so that they would arise against the British. Chief among these conflicts were the two Anglo-Afghan Wars (1839–1842 and 1878–1880), the two Anglo-Sikh Wars (1845–1846 and 1848–1849), and the Indian Mutiny (1857–1858).

The Royal Geographical Society was founded in 1830 and the Imperial Russian Geographical Society in 1845. By mid-century both were fronts for spying expeditions in Asia. Among the earliest of these missions were the journeys of Alexander Burnes (1805–1841) to the Punjab in 1831 and to Bokhara in 1832. John McNeill (1795–1883), a British diplomat in Tehran, published anonymously in 1836 *The Progress and Present Position of Russia in the East*, which bolstered British rationale for keeping a sizeable network of spies in Central Asia.

In the 1830s Conolly was one of the busiest of these "explorers." He was a religious zealot who believed it was Britain's duty to civilize Islamic Central Asia by converting its natives to Christianity. As such, he was a typical hero of Victorian imperialism and "muscular Christianity." The emir of Bokhara would have none of that, and tortured him and Charles Stoddart (1806–1842) in a pit for several months before executing them. The more successful British operatives, such as Burnes, had greater respect for native culture.

On the northwest frontier of India, the British had a staunch ally in Sikh ruler Ranjit Singh (1780–1839), against whom Dost Mohammed (1791–1863), emir of Afghanistan, sought help from Russia. Afghanistan in the 1830s became a diplomatic nightmare for Britain, as the colonial government in Calcutta sought to widen the buffer between India and Russia in this crucial region. Soldiers of

fortune complicated the mix, such as the Italian adventurer Paolo di Avitabile (1791–1850), who ruled Peshawar for the British from 1835 to 1843. In 1837 Henry Rawlinson (1810–1895), en route from Tehran to Herat, happened upon a Russian delegation led by Yan Vitkevitch (d. 1838), headed toward Kabul. The rivals uneasily backed off from each other. Subsequently Vitkevitch was partially successful in sowing anti-British feelings among Dost Mohammed and several other Afghan leaders.

Burnes became the British envoy to Afghanistan in 1836, headquartered in Kabul. Eldred Pottinger (1811–1843) helped the Afghans defend Herat against Russia and Persia in 1837. These two skilled operatives might have been more successful if Burnes had not been placed under the command of Conolly's cousin, William Macnaghten (1793–1841), whose critics described him as "ignorant and tactless." Increasingly distrustful of Dost Mohammed, the British plotted to install Shah Shujah (1780–1842) as puppet ruler of Afghanistan. Macnaghten's bungling prompted the Afghans to rise up and murder Burnes. Macnaghten himself, perhaps the victim of an elaborate plot of entrapment, was murdered by Mohammed Akbar Khan (1818–1847), son of Dost Mohammed, as summary justice for being caught in the act of double dealing with Afghan tribal leaders. The incompetent General William Elphinstone (1782–1842) allowed nearly his entire command to be massacred while retreating from Kabul to Jalalabad.

Besides Kabul, Bokhara, and Herat, several other cities attracted both Russian and British interest, notably Khiva, Khokand, Kashgar, Merv, and Kandahar. James Abbott (1807–1896) journeyed from Herat to Khiva in 1839 and 1840. In 1840 Richmond Campbell Shakespear (1812–1861) persuaded Allah Quli (d. 1842), Khan of Khiva, to free his Russian slaves, probably as much to incite insurrection and destabilize the region as to make a diplomatic or humanitarian gesture.

Count Nikolai Pavlovich Ignatiev (1832–1908) was the leading Russian spymaster in the Great Game. After a series of successful diplomatic missions to China, he served as ambassador to the Ottoman Empire from 1864 to 1877. Utterly ruthless and with keen intuitions about military strategy, he sparked clandestine anti-British operations in India before the mutiny and throughout Central Asia for most of the rest of his career.

In the 1850s France and Britain were both anxious to bolster the sagging Ottoman Empire and thus prevent Russia from gaining unrestricted access to the Mediterranean Sea through the Dardanelles, the Sea of Marmara, and the Bosphorus. Britain knew that Russia's main objective was Constantinople, not Calcutta, but conducted its foreign policy as if Russia desired both. Thus the Crimean War could be seen as part of the Great Game, because it served to divert Russia's attention from India for a while.

Meanwhile the British worked hard, especially in the wake of the Indian Mutiny, to rebuild alliances with native

Asian leaders. These efforts were mostly successful, even though the native rank and file scarcely trusted the British again. Because Persia was allied with Russia, Britain applauded when Dost Mohammed recaptured Herat from the Persians in 1863. Sher Ali (1825–1879), another son of Dost Mohammed, was emir of Afghanistan from 1863 until his death. At first he favored the British, but his gradual shift toward Russia prompted the Second Anglo-Afghan War. The British replaced him with his nephew, Abdur Rahman (1844–1901).

By 1865, Yakub Beg (1820–1877) in Kashgar was the main potentate between China and Russia. Robert Barkley Shaw (1839–1879) and George J. W. Hayward (1840?–1870) made separate trips to Kashgar in 1868, ostensibly to "survey," but really to try to create a British alliance with Yakub Beg. The Russians made similar overtures, but also sent troops to the region under Konstantin Kaufman (1818–1882). Francis Younghusband (1863–1942) led several expeditions through western China, finally entering Lhasa, Tibet, in 1904, ahead of the Russians.

The British grew bolder. Frederick Gustavus Burnaby (1842–1885) dared to travel from St. Petersburg itself to Khiva in 1876. James Thomas Walker (1826–1896), surveyor general of India, ordered more spying expeditions, as did the Russians. By the late 1880s, Britain clearly had the diplomatic advantage in the regions of Central Asia that Russia had not already annexed.

Russian power declined under Czar Nicholas II (1868–1918) in the first decade of the twentieth century. In August, 1907, the Anglo-Russian Convention in St. Petersburg formally ended the Great Game, although the posturing and espionage continued.

## ■ FURTHER READING:

### BOOKS:

- Edwardes, Michael. *Playing the Great Game: A Victorian Cold War*. London: Hamish Hamilton, 1975.
- Hopkirk, Peter. *The Great Game: The Struggle for Empire in Central Asia*. New York: Kodansha International, 1994.
- Ingram, Edward. *The Beginning of the Great Game in Asia: 1828–1834*. Oxford: Clarendon, 1979.
- James, Lawrence. *Raj: The Making and Unmaking of British India*. New York: St. Martin's Griffin, 1997.
- Khan, Munawwar. *Anglo-Afghan Relations, 1798–1878: A Chapter in the Great Game in Central Asia*. Khyber Bazar-Peshawar: University Book Agency, 1963.
- Meyer, Karl Ernest, and Shareen Blair Brysac. *Tournament of Shadows: The Great Game and the Race for Empire in Central Asia*. Washington, D.C.: Counterpoint, 1999.

### SEE ALSO

*Assassination*  
*Geologic and Topographical Influences on Military and Intelligence Operations*

## Greece, Intelligence and Security

Agents of espionage have been employed in the area corresponding to the modern nation of Greece for thousands of years. Spies are mentioned in the works the philosophers and playwrights of ancient Greece, giving the Grecian intelligence community one of the longest lineages and traditions in the world. However, scant comparisons can be drawn between ancient Greece and modern Greece, and their individual employment of intelligence services. Today, Greece maintains a sophisticated civilian intelligence force that utilizes human, signals, communications, and electronic intelligence gathering techniques.

Greece's main intelligence agency is the Hellenic National Intelligence Service (NIS). A recent government reform and restructuring of the Grecian intelligence community expanded the role of the NIS to include both domestic and foreign intelligence operations, and added a counter-terrorism unit to the agency's permanent staff. The NIS is charged with the collection, analysis, and dissemination of intelligence information necessary for the protection of national security. In addition, routine counterintelligence operations, including testing the security of the national communications infrastructure, fall under the jurisdiction of the NIS.

Although the National Intelligence Service is a civilian organization, Greece also maintains limited military intelligence forces, embedded within operational units of the military.

Greece is a member of the North Atlantic Treaty Organization (NATO) and the European Union (EU). Diplomatic negotiations with Turkey over extensive maritime and territorial border disputes are ongoing, but have yielded little consensus between the two nations over national water boundaries in the Aegean Sea. The two nations continue to disagree over the partitioning of neighboring Cyprus.

### ■ FURTHER READING:

#### ELECTRONIC:

Central Intelligence Agency. *The World Factbook*, 2002. "Greece" <<http://www.cia.gov/cia/publications/factbook/geos/gr.html>> (March 30, 2003).

#### SEE ALSO

*NATO (North Atlantic Treaty Organization)*  
*Turkey, Intelligence and Security*

## GSM Encryption

GSM stands for either "group special mobile" or "general system for mobile communications," a protocol or standard for digital cellular communications. GSM encryption is the means by which phone conversations on networks using GSM are scrambled, such that they cannot be descrambled and intercepted by others. Due to their potential uses by terrorist and hostile nations, intelligence agencies in the West are concerned about the dangers inherent in exporting such codes.

In 1982, the European Conference of Post and Telecommunications Administrations adopted the GSM standard, which 18 nations formalized in 1987 with the signing of the GSM Memorandum of Understanding. The first GSM networks began operations in 1991. By the end of the 1990s, some 230 million users worldwide—approximately 65% of the digital wireless market—used digital GSM phones made by companies that included Motorola, Ericsson, and Siemens.

Among the key features of GSM is its security technology, the methods of which reportedly make it the most secure cellular telecommunications standard in the world. Vital to this security is the use of sophisticated encryption algorithms. Conversations are encrypted using a temporary and randomly generated ciphering key, and for added security, the subscriber is identified by a temporary identity, which may change periodically.

Despite these and other advanced security measures, authorities have raised concerns about the safety of GSM codes, and these concerns have been justified by attempts to reveal or break into GSM codes. United States, British, French, and Dutch intelligence and law-enforcement agencies have called for restrictions on the export of encryption technology, which could be used by aggressor nations or terrorists. For example, if terrorists gained encryption codes for cellular telephone communications, they might be able to impede the abilities of law-enforcement authorities to track them and other criminals.

A 1993 compromise permitted the export of the strong A 5/1 encryption algorithm only to secure, fully industrialized countries, mostly in western Europe. The weaker A 5/2 algorithm would be exported to central and eastern Europe, while Russia and some other countries would have no encryption technology.

In April 1998, a group of what *Time* magazine described as "Silicon Valley cypherpunks" hacked into GSM encryption technology, and bragged that they could tap into calls and "clone" other users' cellular phones. A year and a half later, in December 1999, Israeli researchers Alex Biryukov and Adi Shamir announced that they had successfully attacked the A 5/1 algorithm, and claimed that with a modest-sized personal computer, they could penetrate an allegedly secure phone call or data transmission within less than a second. However, an official with the

GSM Association noted that no hardware would allow a hacker to intercept calls on the GSM network.

#### ■ FURTHER READING:

##### PERIODICALS:

Carlson, Caron. "No Threat from GSM Hackers." *Wireless Week* 5, no. 50 (December 13, 1999): 3.

"Firms Are Lining up to See." *Electronic Times* (October 16, 2000): 40.

##### ELECTRONIC:

GSM Association. <<http://www.gsmworld.com>> (March 5, 2003).

##### SEE ALSO

*Computer Hackers  
Encryption of Data  
Telephone Scrambler*

---

## Guatemala, Intelligence and Security

---

Guatemala gained its independence from Spain in 1821. After colonial rule, the region was politically dominated by rival large-land owners. In the latter half of the twentieth century, the government suffered endemic turmoil. Various military coups devastated the national infrastructure, co-opting the nation's small intelligence and security community into political and secret police operations. A 36-year civil war further devastated Guatemala, leaving 100,000 people dead and some one million refugees displaced from their homes.

In 1996, the government issued a peace agreement, formally ending the conflict, but sporadic fighting remains a problem. In peacetime, Guatemala has begun the task of rebuilding its political infrastructure, including its intelligence and security services. New agencies seek to distance themselves from those that operated during the era of political upheaval, but lingering fears of rebel insurgency has prompted the continued use of political espionage against dissidents.

Guatemala's largest intelligence agency is under the direction of the military. The Military Intelligence Wing, D-2, conducts both domestic and foreign intelligence operations. Though D-2 conducts a variety of surveillance missions, a large focus of their operations is the identification and infiltration of paramilitary groups. D-2 also monitors and attempts to stem the trafficking of contraband weapons across national borders.

Guatemala's civilian intelligence community is administered by the Ministry of the Interior and the National

Police. The Ministry of the Interior maintains a sizable investigations and security-intelligence force to combat organized crime, government corruption, and counterfeiting. The National Police are the nation's main law enforcement agency, and maintain their own, specialized intelligence and investigative units.

In recent years, Guatemala has become a major staging area for the trafficking of illegal drugs. The government has joined with others in the region, and the United Nations, to combat the problem, but with varying degrees of success. Government corruption also remain endemic in Guatemala, stifling attempts to rebuild the nation's economy.

#### ■ FURTHER READING:

##### ELECTRONIC:

Central Intelligence Agency. "Guatemala" CIA World Factbook <<http://www.cia.gov/cia/publications/factbook/geos/gt.html>> (April 8, 2003).

---

## Guerilla Warfare

---

#### ■ MARÍA LÓPEZ

In the modern era, guerilla warfare refers to armed resistance by paramilitary or irregular groups toward an occupying force. Guerilla warfare also describes a set of tactics employed by smaller forces against larger, better equipped, and better supplied forces. Guerilla warfare tactics often rely on isolating smaller units of the larger occupying force so as to attack parts of the larger force by ambush. Guerilla forces often practice espionage, industrial sabotage, and wage propaganda campaigns by portraying themselves as a popular but suppressed political movement. In many areas of the world, guerilla warfare is practiced by local groups against government forces, and is especially effective in areas with a rugged natural topography or areas of dense vegetation (e.g., forest or jungle) that provide natural hiding places from which to stage guerilla operations.

Derived from the Spanish term for "little war," guerilla warfare has a long history. Although the term was not used until Spanish partisans resisted the intrusions of Napoleon during the Peninsular War in the early nineteenth century, American colonist revolutionaries practiced guerilla warfare tactics against British forces to win independence from what was arguably the finest military power in the world at the time. During the twentieth century, communist guerilla forces fought successfully against French and then American forces in Vietnam.

Confederate raiders—including Quantrill's raiders (led by William C. Quantrill) and Mosby's raiders (led by John S. Mosby) practiced guerilla warfare against Union forces



A blindfolded Palestinian boy assembles an AK-7 assault rifle, demonstrating skills that he learned at one of the two-week warfare summer camps run by the Palestinian Authority across the West Bank and Gaza in 2000. AP/WIDE WORLD PHOTOS.

during the American Civil War. Following the acquisition of the Philippines after the Spanish-American War, U.S. President Theodore Roosevelt's administration and U.S. forces struggled to suppress Filipino guerilla forces led by Emilio Aguinaldo.

Although usually confined to mountainous or forested terrain, Arab forces inspired by T. E. Lawrence (Lawrence of Arabia) and led by King Faisal al-Husayn used the harsh environment of the desert to fight a successful guerilla war against superior Turkish forces during World War I.

During World War II guerilla forces (also termed "partisan" or "underground" forces) in France and other countries fiercely resisted Nazi occupation.

Well known modern guerilla wars that resulted in permanent changes in government occurred in China, Vietnam, and Cuba. Chinese communist guerillas led by Mao Zedong, prevailed against a number of opponents to eventually take power after WWII. Communist Viet Minh forces led by Ho Chi Minh and later Viet Cong guerilla forces outlasted French and then American forces in Vietnam. In Cuba, Fidel Castro and Ernesto (Che) Guevara fought a three year long guerilla war from 1956 to 1959 that eventually ousted the launched a guerilla war in Cuba against the government of Fulgencio Batista.

Guevara's writings became politically influential for a number of guerilla groups that organized across Central and South America. Guevara wrote that "popular forces can win a war against (an) army" and that "it (was) not necessary to wait until all conditions for making revolution exist; the insurrection can create them."

Other nationalist movements sprung from guerilla movement roots in Algeria (against the French in 1954); Cyprus (Greek nationalists against the British in the late 1950s).

Although often portraying themselves as a popular front, guerilla forces seizing power often engage in bloody "cleansing" and destruction of local populations once loyal to the former government. After seizing power in Cambodia, the Khmer Rouge led by Pol Pot (also known as Soloth Sar) killed an estimated two million Cambodians.

Although sometimes only a matter of semantics, there is often considerable debate concerning the overlap of guerilla tactics with tactics employed by terrorists (e.g., hijacking, kidnapping). There are no easily agreed upon definitional lines to distinguish the two groups. In general, most historians hinge such distinctions not necessarily upon tactics employed, but rather on relations between the opposing parties and the targets selected. Although there are many historical exceptions, terrorists generally represent minority or extreme viewpoints and target civilian, military, or government targets. Guerilla forces generally represent broader popular movements and generally attack occupying military or government forces. A key element in defining guerilla forces as opposed to other types of forces or movements involves the general principle that guerilla forces are generally accepted—in fact often supported and sheltered—by local populations. In accord with international law, in stark contrast to the legal treatment of terrorist groups, guerilla forces are to be treated as combatants in accord with the rules of the Geneva Convention if the forces operate in uniform or carry as distinctive emblem (e.g., patch, red scarf, etc.).

In many cases, whether to declare a particular group a group of freedom fighters, a guerilla force, or a terrorist organization is often a matter of political or geographical perspective.

Cyberspace opens new opportunities and perils for what may come to be considered a new form of guerilla warfare in the twenty-first century as activists (also known as "hacktivists") use Internet technology to combat electronic monitoring and Internet censorship by governments in many parts of the world.

#### SEE ALSO

*Terrorist and Para-State Organizations*

*This page intentionally left blank*



## Hackers.

SEE *Computer Hackers*.

---

## HAMAS (Islamic Resistance Movement)

---

HAMAS was formed in late 1987 as an outgrowth of the Palestinian branch of the Muslim Brotherhood. Various HAMAS elements have used both political and violent means, including terrorism, to pursue the goal of establishing an Islamic Palestinian state in place of Israel. HAMAS is loosely structured, with some elements working clandestinely and others working openly through mosques and social service institutions (including charities organized by HAMAS) to recruit members, raise money, organize activities, and distribute propaganda. HAMAS' strength is concentrated in the Gaza Strip and a few areas of the West Bank. HAMAS also has engaged in political activity, such as running candidates in West Bank Chamber of Commerce elections.

**Organization activities.** HAMAS is a large organization with tens of thousands of supporters and sympathizers. HAMAS activists, especially those in the Izz el-Din al-Qassam Brigades, have conducted many attacks—including large-scale suicide bombings—against Israeli civilian and military targets. In the early 1990s, HAMAS also targeted Fatah rivals and began a continuing practice of targeting suspected Palestinian collaborators. HAMAS increased operational activity in 2001 during the Intifadah, claiming numerous attacks against Israeli interests. HAMAS has not directly targeted U.S. interests and continues to confine its attacks to Israelis inside Israel and the territories.

HAMAS operates primarily in the West Bank, Gaza Strip, and Israel. In August 1999, Jordanian authorities closed the group's Political Bureau offices in Amman, arrested its leaders, and prohibited the group from operating on Jordanian territory. HAMAS leaders are also present in other parts of the Middle East, including Syria, Lebanon, and Iran.

HAMAS receives funding from Palestinian expatriates, Iran, and private benefactors in Saudi Arabia and other moderate Arab states. Some fundraising and propaganda activity take place in Western Europe and North America.

### ■ FURTHER READING:

#### ELECTRONIC:

Central Intelligence Agency. *World Factbook*, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. *Patterns of Global Terrorism 2001, Annual Report: On the Record Briefing*. May 21, 2002 <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. *Annual Reports*. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

#### SEE ALSO

*Terrorism, Philosophical and Ideological Origins*  
*Terrorist and Para-State Organizations*  
*Terrorist Organization List, United States*  
*Terrorist Organizations, Freezing of Assets*

---

## Hanssen (Robert) Espionage Case

---

### ■ ADRIENNE WILMOTH LERNER

Robert Phillip Hanssen, a 25-year FBI veteran, was one of the most successful double agents to ever steal secrets



Photo released by the FBI February 20, 2001, showing FBI agent Robert Philip Hanssen, who was arrested under the accusation of spying for Russia. ©AFP/CORBIS.

from the United States government. Hanssen used his position in the FBI to sell classified information to the Soviet KGB and later Russian Intelligence. A complex and often contradictory portrait emerged in the 109-page federal affidavit that detailed Hanssen's activities. The FBI alleged that Hanssen intentionally stole secret documents and sold them for private financial gain to the KGB over a period of 15 years. Like most double agents, a different social portrait of the man emerged. Friends, neighbors, and family described Hanssen as quiet, frugal, and devout.

Born in April 1944, Hanssen was the only child of Vivian and Howard Hanssen, a Chicago police lieutenant. He studied Russian and earned degrees in chemistry. After flirting with various career interests, Hanssen joined the Chicago Police Department in October, 1972. His first post was in a new undercover unit called C-5, which sought out corrupt police officers.

Hanssen's intelligence and ability stood out even in the elite C-5 group. A colleague suggested he join the FBI. On January 12, 1976, he joined the FBI, working in Indiana and New York City before being transferred to the Washington, D.C., headquarters in 1981. He initially tracked white-collar crime and monitored foreign officials assigned to the United States. Hanssen also spent two years as a member of a high-level analytical unit that monitored Soviet intelligence. While working as an analyst, Hanssen

gathered and copied classified materials and began making contact with the Soviet KGB.

In 1985, Hanssen transferred to the FBI's Manhattan bureau to head a foreign counterintelligence squad. At that post, Hanssen could more readily funnel information to his Soviet handlers. Though his motives remained unclear, within nine days of joining the New York office Hanssen allegedly mailed a letter to the KGB offering stolen classified documents in exchange for \$100,000. Over the next 15 years, with varying frequency, Hanssen sold information to rival foreign intelligence services.

In February 2000, Hanssen was arrested on espionage charges at a "dead drop" at a park near his home. The FBI accused him of receiving more than \$600,000 in cash and diamonds for delivering 6,000 pages of documents and 26 computer discs to his Russian handlers. It was also alleged that \$800,000 more was waiting for him in a Moscow bank. The FBI built its case against Hanssen by collecting, from unidentified sources, packages that bore Hanssen's fingerprints, and the apparent KGB file on Hanssen, which detailed his drops and letters to the Russian intelligence agency. Upon further investigation, the FBI compiled evidence of Hanssen's decades-long career as a double agent.

On May 10, 2002, Hanssen was sentenced to life in prison without the possibility of parole. In his trial, he plead guilty to all counts of espionage and conspiracy that were levied against him.

#### ■ FURTHER READING:

##### ELECTRONIC:

The Center for Counterintelligence and Security Studies. <[http://www.cicentre.com/Documents/DOC\\_Hanssen\\_1.htm](http://www.cicentre.com/Documents/DOC_Hanssen_1.htm)> (April 2003).

United States Federal Bureau of Investigation. <<http://www.fbi.gov/libref/historic/famcases/hanssen/hanssen.htm#anchor26782>> (April 2003).

##### SEE ALSO

*Ames (Aldrich H.) Espionage Case*

*Dead Drop Spike*

*Dead-Letter Box*

*FBI (United States Federal Bureau of Investigation)*

*KGB (Komitet Gosudarstvennoi Bezopasnosti, USSR Committee of State Security)*

*Russia, Intelligence and Security*

---

## Harakat ul-Jihad-I-Islami (HUJI) (Movement of Islamic Holy War)

---

Harakat ul-Jihad-I-Islami (HUJI)—Movement of Islamic Holy War—is a Sunni extremist group that follows the



Deobandi tradition of Islam, and was founded in 1980 in Afghanistan to fight in the Jihad against the Soviets. It is also affiliated with the Jamiat Ulema-I-Islam Fazlur Rehman faction (JUI-F) and the Deobandi school of Sunni Islam. The group, led by chief commander Amin Rabbani, is made up primarily of Pakistanis and foreign Islamists who are fighting for the liberation of Kashmir and its accession to Pakistan. HUJI has conducted a number of operations against Indian military targets in Kashmir, and are linked to the Kashmiri militant group al-Faran that kidnapped five Western tourists in Kashmir in July 1995; one was killed in August 1995 and the other four reportedly were killed in December of the same year.

HUJI strength is unknown, but intelligence services estimate that there may be several hundred members operating in Pakistan and Kashmir. HUJI trained members in Afghanistan until Operation Enduring Freedom began in the fall of 2001.

#### ■ FURTHER READING :

##### ELECTRONIC:

CDI (Center for Defense Information), Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <<http://www.cdi.org/terrorism/terrorist.cfm>> (April 17, 2003).

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001," Annual Report: On the Record Briefing. May 21, 2002 <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual Reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

##### SEE ALSO

*Terrorism, Philosophical and Ideological Origins Terrorist and Para-State Organizations Terrorist Organization List, United States Terrorist Organizations, Freezing of Assets*

connections to the Pakistani militant groups Harakat ul-Jihad-I-Islami (HUJI) and Harakat ul-Mujahidin (HUM), who advocate similar objectives in Pakistan and Kashmir. HUJI-B was accused of stabbing a senior Bangladeshi journalist in November, 2000, for making a documentary on the plight of Hindus in Bangladesh. HUJI-B was suspected in the July 2000, assassination attempt of Bangladeshi Prime Minister Sheikh Hasina.

HUJI-B has an estimated cadre strength of several thousand members and operates and trains members in Bangladesh, where it maintains at least six camps. Funding of the HUJI-B comes primarily from madrassas in Bangladesh. The group also has ties to militants in Pakistan that may provide another funding source.

#### ■ FURTHER READING :

##### ELECTRONIC:

CDI (Center for Defense Information), Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <<http://www.cdi.org/terrorism/terrorist.cfm>> (April 17, 2003).

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001," Annual Report: On the Record Briefing. May 21, 2002 <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual Reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

##### SEE ALSO

*Terrorism, Philosophical and Ideological Origins Terrorist and Para-State Organizations Terrorist Organization List, United States Terrorist Organizations, Freezing of Assets*

---

## Harakat ul-Mujahidin (HUM) (Movement of Holy Warriors)

---



---

## Harakat ul-Jihad-I-Islami/ Bangladesh (HUJI-B) (Movement of Islamic Holy War)

---

The mission of Harakat ul-Jihad-I-Islami/Bangladesh (HUJI-B) (Movement of Islamic Holy War), led by Shauqat Osman, is to establish Islamic rule in Bangladesh. HUJI-B has

The Harakat ul-Mujahidin is an Islamic militant group based in Pakistan that operates primarily in Kashmir. It is politically aligned with the radical political party, Jamiat Ulema-I Islam Fazlur Rehman faction (JUI-F). Long-time leader of the group, Fazlur Rehman Khalil, in mid-February 2000 stepped down as HUM emir, turning the reins over to the popular Kashmiri commander and his second-in-command, Farooq Kashmiri. Khalil, who has been linked to Osama Bin Ladin and signed his fatwa in February 1998 calling for attacks on United States and Western interests, assumed the position of HUM Secretary General.

HUM operated terrorist training camps in eastern Afghanistan until Coalition airstrikes destroyed them during the Fall of 2001.

**Organization activities.** HUM has conducted a number of operations against Indian troops and civilian targets in Kashmir. HUM also has been linked to the Kashmiri militant group al-Faran that kidnapped five Western tourists in Kashmir in July 1995—one was killed in August 1995 and the other four reportedly were killed in December of the same year. The HUM is responsible for the hijacking of an Indian airliner on December 24, 1999, that resulted in the release of Masood Azhar—an important leader in the former Harakat ul-Ansar imprisoned by the Indians in 1994—and Ahmad Omar Sheikh, who was arrested for the abduction and murder in January-February 2001 of U.S. journalist Daniel Pearl.

HUM is based in Muzaffarabad, Rawalpindi, and several other towns in Pakistan, but members conduct insurgent and terrorist activities primarily in Kashmir. The HUM trained its militants in Afghanistan and Pakistan. They have several thousand armed supporters located in Azad Kashmir, Pakistan, and India's southern Kashmir and Doda regions. Supporters are mostly Pakistanis and Kashmiris and also include Afghans and Arab veterans of the Afghan war. HUM uses light and heavy machine guns, assault rifles, mortars, explosives, and rockets. HUM lost a significant share of its membership in defections to the Jaish-e-Mohammed (JEM) in 2000.

HUM collects donations from Saudi Arabia and other Gulf and Islamic states and from Pakistanis and Kashmiris. The HUM's financial collection methods also include soliciting donations through magazine ads and pamphlets. The sources and amount of HUM's military funding are unknown. In anticipation of asset seizures by the Pakistani Government, the HUM withdrew funds from bank accounts and invested in legal businesses, such as commodity trading, real estate, and production of consumer goods. Its fundraising in Pakistan has been constrained since the government clampdown on extremist groups and freezing of terrorist assets.

#### ■ FURTHER READING:

##### ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001, Annual Report: On the Record Briefing. May 21, 2002 <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

##### SEE ALSO

*Terrorism, Philosophical and Ideological Origins*

*Terrorist and Para-State Organizations*  
*Terrorist Organization List, United States*  
*Terrorist Organizations, Freezing of Assets*

## Hardening

In a general sense, hardening is the process of securing a computer. More specifically, hardening is the removal or disabling of all components in a computer system that are not necessary to its principal function or functions. By reducing the purposes for which a computer is used, the computer is rendered less vulnerable to outside attack by hackers or other intruders.

General hardening steps include limiting the number of users allowed to access a computer, tightening password and access control, and installing basic intrusion-detection software. The more specific variety of hardening requires the involvement of a highly trained computer technician. Once the user has defined the principal purpose or purposes for which the computer is to be used, then the technician can disable or remove all components that are not necessary to those purposes.

An example of a computer that needs to be hardened is a server, a computer, or device on a network (a group of linked computers) that manages network resources. The server should be equipped with high-quality firewall software to prevent outside intrusion. Often, such software may not provide enough security, in which case hardening is necessary. If the server is properly hardened, this narrows the avenues of access for intruders hoping to get past the server to other computers on the local network.

During the hardening process, a computer should be disconnected from any network. Once it is hardened, the computer will no longer be a general-purpose machine, but will be usable only for the very specific purposes for which it has been designated. The more specific that purpose, and the fewer general-purpose features on the computer, the more difficult it will be for a would-be intruder to access the computer, or to use it effectively once it has been accessed.

#### ■ FURTHER READING:

##### BOOKS:

Akin, Thomas. *Hardening Cisco Routers*. Sebastopol, CA: O'Reilly, 2002.

##### PERIODICALS:

Connolly, P. J. "Fight DDoS Attacks with Intelligence." *InfoWorld* 23, no. 39 (September 24, 2001): 58.

Levine, Bernard. "What's Next for Electronics?" *Electronic News* 47, no. 40 (October 1, 2001): 1.

Wang, Wallace. "Hardening Your System." *Boardwatch* 15, no. 8 (June 2001): 44–46.

#### SEE ALSO

*Computer Hackers*  
*Computer Hardware Security*  
*Computer Software Security*

## Health and Human Services Department, United States

The United States Department of Health and Human Services (HHS) is responsible for overseeing government departments and programs devoted to public health. The HHS manages federal health insurance programs Medicare and Medicaid for certain citizens. Other operational departments within the HHS have a direct impact on general matters of national security, public safety, and counter-terrorism.

The HHS currently oversees over 300 various programs and has an annual operating budget of around 460 billion dollars. The department was founded in the 1930s as part of the New Deal, but has since grown in scope to cover everything from preschool programs to medical research.

Two main branches of the HHS are especially important to the preservation of national security. The Food and Drug Administration (FDA) is responsible for pharmaceutical research and the approval of medicines for sale and distribution in the United States. The FDA also regulates some aspects of agriculture and insures the safety of food products for consumers. Working with the Environmental Protection Agency, the FDA helped to establish guidelines for drinking water treatment and regulation. Food safety, water purity, and drug research and approval have increased in importance in recent years since America has come under terrorist threat. The FDA sponsors research into protecting food and water systems from bioterrorism attacks. Other research funding supports the development and testing of vaccines and drugs to fight diseases that are most likely to be used in such an attack.

Perhaps the most important organizational branch of the HHS in terms of national security, as well as public health, is the Centers for Disease Control and Prevention (CDC). The CDC, located in Atlanta, Georgia, is the primary disease research facility in the world and monitors the spread of epidemic diseases whether natural or the result of bioterrorism. The CDC has introduced several new initiatives to investigate, plan for, and combat bioterrorism and radiological attacks. Constant research on disease virulence, transmission, and treatments insures that most diseases are readily identifiable. Several instances in the

past, including the September 11th terrorist attacks on the United States, have prompted the CDC to issue advisories to doctors on symptoms of diseases that can be the result of bioterrorism. The CDC stressed that some of these diseases could be difficult to diagnose because they had been eradicated from the United States for decades. Also, the organization released information to the general public regarding the best ways to prepare for and survive a biological or radiological attack.

The HHS, with the aid of the CDC, also administers general and emergency vaccination and inoculation programs, including advising the military on possible health threats that could be encountered abroad. Individual state bioterrorism readiness plans must also be approved by the HHS.

#### ■ FURTHER READING:

##### ELECTRONIC:

Centers for Disease Control "Bioterrorism Preparedness." <<http://www.bt.cdc.gov/>> (November 28, 2002).

#### SEE ALSO

*CDC (United States Centers for Disease Control and Prevention)*

## Heavy Water Technology

#### ■ LARRY GILMAN

Heavy water is water (H<sub>2</sub>O) in which oxygen is bound to atoms of the hydrogen isotope deuterium (<sup>2</sup>H). Heavy water is so named because it is significantly more dense (>1.1 g/cm<sup>3</sup>) than ordinary ("light") water, <sup>1</sup>H<sub>2</sub>O (1 gm/cm<sup>3</sup>). Heavy water is not radioactive and has the same chemical properties as light water; a person could drink a glass of heavy water without harm. However, heavy water is better than light water at moderating (slowing) neutrons, which makes it useful in some nuclear reactor cores. Its scarcity during World War II, partly assured by bombing raids and daring Allied commando missions to destroy heavy-water production facilities, interfered critically with the German and Japanese nuclear programs.

**Deuterium and tritium.** All hydrogen atoms have atomic number 1, that is, one proton in the nucleus; common or light hydrogen also has mass number 1, that is, its nucleus consists solely of a lone proton. Deuterium (<sup>2</sup>H) has atomic number 1 and mass number 2, because its nucleus contains one proton plus one neutron. The presence of the neutrons in the deuterium atoms of heavy water is what

makes it “heavy” (i.e., more dense than common water). Tritium ( $^3\text{H}$ ) is an isotope of hydrogen whose nuclei contain one proton plus two neutrons. Tritium can also combine with oxygen to form heavy water, but tritium is much rarer than deuterium, so virtually all heavy water consists of  $^2\text{H}_2\text{O}$  (deuterium oxide). Tritium heavy water is radioactive and has been used as a tracer in certain biological experiments.

About .015% of the hydrogen atoms in natural water are deuterium atoms. Heavy water is produced by using electricity to break up water molecules, releasing its hydrogen as gas. (This process is known as electrolysis.) Deuterium oxide molecules are more resistant to electrolysis than light-water molecules, so electrolysis of a volume of water tends to increase its concentration of heavy water. By repeated concentration steps, almost pure heavy water can be obtained. Heavy water can also be extracted from natural water by repeated evaporation steps, as its heavier molecules are less volatile than those of light water (i.e., less likely to gain enough kinetic energy in random molecular collisions to leave the surface of a liquid mass). The electrolysis method was important during World War II, but evaporation methods are used today because they are less expensive.

**Neutron moderation.** The utility of heavy water in nuclear reactors arises from its ability to slow down or moderate neutrons. Slow or thermal neutrons are more likely to cause unstable nuclei (e.g., of uranium) to fission upon impact; however, neutrons emitted by fissioning nuclei generally have high velocities. To make a nuclear chain reaction sustainable, therefore, it is often desirable to slow down or moderate neutrons released by fissioning nuclei. Slowed-down neutrons are termed thermal neutrons, and reactors that employ a moderator to produce thermal neutrons are termed thermal reactors. (Other reactor designs are also possible.) Interposing a neutron-slowing substance or moderator between thin rods filled with nuclear fuel is a common feature of thermal reactor cores. Most of the neutrons released by fissioning nuclei in the fuel rods escape quickly from the thin rods and collide with atoms in the moderator before passing into other fuel rods; these collisions impart some of the neutrons’ kinetic energy to atoms in the moderator. This heats the moderator, and some of the slowed neutrons go on to enter fuel rods and to cause nuclei to fission in them.

Several substances have been used as moderators in nuclear reactors, especially carbon (in the form of graphite), light water, heavy water, and beryllium. Heavy water is a desirable moderator for several reasons. It has excellent moderation properties and, being a liquid, can act simultaneously as a coolant to transfer heat out of the core to a power-generation loop.

Today, most power-generating reactors in the world utilize light water as a moderator. Light water has less desirable moderation properties than heavy water, but the

fact that it is essentially free, while heavy water is expensive, gives it an advantage. However, one class of modern reactor—the Canadian CANDU (CANada Deuterium Uranium) reactor type—uses heavy water as a moderator. A CANDU reactor core consists of a stack of horizontal fuel-rod assemblies immersed in a large holding tank full of heavy water that serves to reduce stray radiation in the vicinity of the unit. Hot heavy water circulates through tubes stacked between the fuel-rod assemblies, acting both to moderate neutrons in the core and to carry away heat energy. The circulating heavy water is under high pressure to keep it from flashing to steam. After being heated in the reactor core, it is passed through a heat exchanger, a device which allows hot water to circulate on one side of a thin metal barrier and relatively cool water to circulate on the other; heat is conducted through the metal from the hotter to the cooler water, which is then pumped away and allowed to expand into steam to drive turbines. The turbines, in turn, drive generators that make electricity.

**Heavy water during World War II.** During the early days of nuclear fission, in the 1930s and early 1940s, scientists struggled with what is today a routine task: the production of a sustained, controlled nuclear chain reaction in a reactor core. It took intense research to discover that a moderator was required at all. Graphite was known to be a good moderator, and some of the earliest nuclear reactors consisted of large piles of graphite blocks riddled with pellets of nuclear fuel. However, heavy water was easier to handle and had superior moderation properties; rapid progress in nuclear fission, given the state of knowledge at that time, required heavy water.

However, heavy water was rare. The only commercial producer of heavy water in the world in the late 1930s was Norsk Hydro, the state-owned Norwegian hydroelectric company. In 1940, the Germans invaded and occupied Norway, seizing the heavy-water production facility at Rjukan-Vemork, Norway. By 1942, U.S. intelligence was aware that the German nuclear research program was using heavy water produced using the electrolysis method at Rjukan-Vemork. In November 1942, British commandos (special forces trained to operate in small numbers behind enemy lines) attempted to land in Norway and destroy essential machinery at Rjukan-Vemork; they were all killed in crashes or captured and executed by the Germans. (Hitler had ordered that all captured commandos were to be shot.) In February 1943, a second commando raid was attempted. This raid succeeded in putting the Rjukan-Vemork heavy-water plant temporarily out of commission. All commandos involved escaped, and the German fission program was delayed by some months. However, the facility was repaired and put back into operation. In November 1943, a force of 460 U.S. bombers was dispatched from England to bomb the Norwegian plant. Not all essential heavy-water machinery at the site was destroyed, but the German government decided to move what was left, including whatever stocks of heavy water

had been accumulated, to Germany, where they could be better defended. However, Norwegian resistance personnel succeeded in sinking the ferry that was to carry the precious barrels of heavy water across a lake on its way to Germany, further impeding German nuclear efforts. In the months remaining before the Germans were defeated they could not produce sufficient quantities of heavy water, and their nuclear program (which was mostly devoted to the goal of producing electricity, rather than a nuclear bomb) did not succeed. The extreme scarcity of heavy water in Japan was also a factor in that country's decision not to pursue development of nuclear explosives during World War II.

#### ■ FURTHER READING:

##### BOOKS:

- Dahl, Per F. *Heavy Water and the Wartime Race for Nuclear Energy*. Bath, UK: Institute of Physics Publishing, 1999.
- Glasston, Samuel, and Alexander Sesonske. *Nuclear Reactor Engineering: Vol. 1, Reactor Design Basics*. New York: Chapman & Hall, 1994.

##### SEE ALSO

*Chemistry: Applications in Espionage, Intelligence, and Security Issues*  
*Manhattan Project*  
*Nuclear Power Plants, Security*  
*Nuclear Reactors*  
*Nuclear Weapons*

## Hemorrhagic Fevers and Diseases

■ BRIAN D. HOYLE

Hemorrhagic diseases are caused by infection with viruses or bacteria. As the name implies, a hallmark of a hemorrhagic disease is copious bleeding. The onset of a hemorrhagic fever or disease can lead to relatively mild symptoms that clear up within a short time. However, hemorrhagic diseases are most recognized because of the ferocity and lethality of their symptoms as well as the speed at which they render a person extremely ill.

High rates of infection, easy transmission, and high levels of morbidity (illness) and mortality (death) mean that some hemorrhagic viruses hold the potential for use as biological weapons. Viruses including, but not limited, Ebola, Marburg, Lassa fever, and New World arenaviruses, offer characteristics desirable in potential bioweapon agents.

**Four groups of hemorrhagic viruses.** The viruses that cause hemorrhagic diseases are members of four groups. These are the arenaviruses, filoviruses, bunyaviruses, and the flaviviruses. Arenaviruses are the cause of Argentine hemorrhagic fever, Bolivian hemorrhagic fever, Sabia-associated hemorrhagic fever, Lassa fever, Lymphocytic choriomeningitis, and Venezuelan hemorrhagic fever. The bunyavirus group causes Crimean-Congo hemorrhagic fever, Rift Valley fever, and Hantavirus pulmonary syndrome. Filoviruses are the cause of Ebola hemorrhagic fever and Marburg hemorrhagic fever. Lastly, the flaviviruses cause tick-borne encephalitis, yellow fever, Dengue hemorrhagic fever, Kyasanur Forest disease, and Omsk hemorrhagic fever.

Virtually all the hemorrhagic diseases of microbiological origin that arise with any frequency are caused by viruses. The various viral diseases are also known as viral hemorrhagic fevers. Bacterial infections that lead to hemorrhagic fever are rare. One example is a bacterium known as scrub typhus.

None of the known viral hemorrhagic diseases are indigenous to the United States (i.e., none occur naturally). Accordingly, a primary risk factor of viral hemorrhagic diseases includes travel to areas where the virus is indigenous (e.g., portions of Africa, Asia, the Middle East, and South America).

Work with these viruses must only be conducted in high containment (BSL-4) laboratories. There are two such labs in the U.S.; one is located at the Centers for Disease Control and Prevention (CDC), and the other at the United States Army Medical Research Institute of Infectious Diseases (USAMRIID). All personnel at these laboratories must wear protective clothing (e.g., double-gloves, biohazard suits, shoe coverings, face shields, respirators, etc.) and often work in negative pressure rooms.

Although Ribavirin, an antiviral medication, has shown some effectiveness against arenaviridae and bunyaviridae viruses, there are currently no antiviral medications effective against filoviridae and flaviviridae viruses. A vaccine exists for only yellow fever. Insect vectors are controlled by a concerted campaign of spraying and observance of precautionary measures (e.g., use of insect repellent, proper clothing, insect netting over sleeping areas, etc.).

**Molecular biology and modes of transmission.** While the viruses in the groups display differences in structure and severity of the symptoms they can cause, there are some features that are shared by all the viruses. For instance, all the hemorrhagic viruses contain ribonucleic acid as their genetic material. The nucleic acid is contained within a so-called envelope that is typically made of lipids. Additionally, all the viruses require a host in which to live. The animal or insect that serves as the host is also called the natural reservoir of the particular virus. This natural reservoir does not include humans. Infection of humans occurs only incidentally upon contact with the natural reservoir.

Symptoms of hemorrhagic diseases can progress from mild to catastrophic in only hours. As a result, an outbreak of hemorrhagic disease tends to be self-limiting in a short time. In some cases, this is because the high death rate of those who are infected literally leaves the virus with no host to infect. Often the outbreak fades away as quickly as it appeared.

Hemorrhagic-fever-related illnesses appear in a geographical area where the natural reservoir and humans are both present. If the contact between the two species is close enough, then the disease-causing microorganism may be able to pass from the species that is the natural reservoir to the human.

Although little is clear about the state of the microbes in their natural hosts, it is reasonably clear now that the viruses do not damage these hosts as much as they do a human who acquires the microorganisms. Clarifying the reasons for the resistance of the natural host to the infections would be helpful in finding an effective treatment for human hemorrhagic diseases.

The speed at which hemorrhagic fevers appear and end in human populations, combined with their frequent occurrence in relatively isolated areas of the globe has made detailed study difficult. Even though some of the diseases, such as Argentine hemorrhagic fever, have been known for almost 50 years, knowledge of the molecular basis of the disease is lacking. For example, while it is apparent that some hemorrhagic viruses can be transmitted through the air as aerosols, the pathway of infection once the microorganism has been inhaled is still largely unknown.

The transmission of hemorrhagic viruses from the animal reservoir to humans makes the viruses the quintessential zoonotic disease. For some of the viruses, the host has been determined. Hosts include the cotton rat, deer mouse, house mouse, arthropod ticks, and mosquitoes. However, for other viruses, such as the Ebola and Marburg viruses, the natural host still remains undetermined. Outbreaks with the Ebola and Marburg viruses have involved transfer of the virus to humans via primates. Whether the primate is the natural host or acquired the virus as the result of contact with the true natural host is not clear.

Another fairly common feature of hemorrhagic diseases is that once humans are infected with the agent of the disease, human-to-human transmission can occur. Often this transmission is via body fluids that accidentally contact a person who is offering care to the afflicted person.

Hemorrhagic diseases typically begin with a fever, a feeling of tiredness, and aching muscles. These symptoms may not progress further, and recovery may occur within a short time. However, damage that is more serious often is characterized by copious bleeding, especially from orifices such as the mouth, eyes, and ears. More seriously, internal bleeding also occurs as organs are attacked by the infection. Death can result, though usually not from direct loss of blood, but from nervous system failure, coma, or seizures.

## ■ FURTHER READING:

### BOOKS:

Andreoli, Thomas E., et al. *Cecil Essentials of Medicine*. Philadelphia: W. B. Saunders, 1993.

Cormican, M. G., and M. A. Pfaller. "Molecular Pathology of Infectious Diseases," in *Clinical Diagnosis and Management by Laboratory Methods*. 20th ed. Philadelphia: W. B. Saunders, 2001.

### PERIODICALS:

Dutton, Gail. "Biotechnology Counters Bioterrorism." *Genetic Engineering News* no. 21 (December 2000): 1–22ff.

Peters, C. J., and J. W. LeDuc. "An Introduction to Ebola: The Virus and the Disease." *The Journal of Infectious Diseases* no. 179 (Supplement 1, February 1999): ix–xvi.

### ELECTRONIC:

Centers for Disease Control. "Ebola Hemorrhagic Fever." 2001. <<http://www.cdc.gov/ncidod/dvrd/spb/mnpages/dispages/ebola.htm>> (March 12, 2003).

Centers for Disease Control. "Viral Hemorrhagic Fevers." 2000. <<http://www.cdc.gov/ncidod/dvrd/spb/mnpages/dispages/vhf.htm>> (March 12, 2003).

Centers for Disease Control. "Yellow Fever: Disease and Vaccine." 2001. <<http://www.cdc.gov/ncidod/dvbid/yellowfever/index.htm>> (March 12, 2003).

### SEE ALSO

*Biological Warfare*  
*Biological Weapons, Genetic Identification*  
*Bioshield Project*  
*Bioterrorism*  
*Bioterrorism, Protective Measures*  
*CDC (United States Centers for Disease Control and Prevention)*  
*Chemical and Biological Detection Technologies*

---

## Hizballah (Party of God)

---

Hizballah (Party of God) (also operates as, or is known as: Islamic Jihad, Revolutionary Justice Organization, Organization of the Oppressed on Earth, and Islamic Jihad for the Liberation of Palestine) was formed in 1982 in response to the Israeli invasion of Lebanon. This Lebanon-based radical Shi'a group takes its ideological inspiration from the Iranian revolution and the teachings of the Ayatollah Khomeini. The Majlis al-Shura, or Consultative Council, is the group's highest governing body and is led by Secretary General Hassan Nasrallah. Hizballah formally advocates ultimate establishment of Islamic rule in Lebanon and liberating all occupied Arab lands, including Jerusalem. Hizballah has expressed as a goal the elimination of Israel. Hizballah has also expressed its unwillingness to

work within the confines of Lebanon's established political system; however, this stance changed with the party's decision in 1992 to participate in parliamentary elections. Although closely allied with and often directed by Iran, the group may have conducted operations that were not approved by Tehran. While Hizballah does not share the Syrian regime's secular orientation, the group has been a strong tactical ally in helping Syria advance its political objectives in the region.

**Organization activities.** Hizballah is known or suspected to have been involved in numerous anti-U.S. terrorist attacks, including the suicide truck bombings of the U.S. Embassy in Beirut in April 1983, the U.S. Marine barracks in Beirut in October 1983, and the U.S. Embassy annex in Beirut in September 1984. Three members of Hizballah, 'Imad Mughniyah, Hasan Izz-al-Din, and Ali Atwa, have been on the FBI's list of the 22 most wanted terrorists for the hijacking in 1985 of TWA Flight 847 during which a U.S. Navy diver was murdered. Elements of Hizballah were responsible for the kidnapping and detention of U.S. and other Western hostages in Lebanon. The group also attacked the Israeli Embassy in Argentina in 1992 and is a suspect in the 1994 bombing of the Israeli cultural center in Buenos Aires. In fall 2000, it captured three Israeli soldiers in the Shabaa Farms and kidnapped an Israeli noncombatant whom it may have lured to Lebanon under false pretenses.

Hizballah is known to have several thousand supporters and a few hundred terrorist operatives operating in the Bekaa Valley, Hermil, the southern suburbs of Beirut, and southern Lebanon. They have established cells in Europe, Africa, South America, North America, and Asia.

Hizballah receives substantial amounts of financial, training, weapons, explosives, political, diplomatic, and organizational aid from Iran and received diplomatic, political, and logistical support from Syria.

#### ■ FURTHER READING:

##### ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001, Annual Report: On the Record Briefing. May 21, 2002 <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual Reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

##### SEE ALSO

*Terrorism, Philosophical and Ideological Origins*  
*Terrorist and Para-State Organizations*  
*Terrorist Organization List, United States*  
*Terrorist Organizations, Freezing of Assets*

## Holocaust Art Theft.

SEE *Archeology and Artifacts, Protection of during War.*

## Homeland Security, United States Department of

### ■ JUDSON KNIGHT

The Department of Homeland Security (DHS) is a direct outgrowth of the terrorist attacks on September 11, 2001, which highlighted America's vulnerability to terrorism. Initiated by President George W. Bush as the Office of Homeland Security, the DHS became fully operational in 2003. The DHS incorporates several dozen offices and agencies, many of them previously assigned to other departments and some entirely new. They include the U.S. Coast Guard (USCG), U.S. Secret Service (USSS), Federal Emergency Management Agency (FEMA), Immigration and Naturalization Service (INS), and the newly created Transportation Security Administration (TSA). These and many other bureaus would be placed under, or work in tandem with, one of the five DHS directorates—Border and Transportation Security, Emergency Preparedness and Response, Science and Technology, Information Analysis and Infrastructure Protection, and Management—to fulfill the greater DHS mission of preventing, mitigating, and protecting against terrorism on U.S. soil.

## Civil Defense and Homeland Security

Prior to September 11, 2001, what Americans now refer to as "homeland security"—protection of the nation, its people, its land, and its resources from attack—bore a different name: civil defense. The civil defense concept had its origins in World War II, when Americans organized local groups to prepare for and protect against the threat of Axis attack on American shores. This concept carried over into the Cold War, with a few changes; the enemy was now the Soviet Union, and the threat had the dimensions of nuclear annihilation.

In the early 1960s, the heyday of Cold War civil defense efforts, some American families built bomb shelters, and students practiced "duck and cover" maneuvers that would supposedly protect them in the event of a nuclear attack. A decade later, however, with the Cuban Missile



Homeland Security Director Tom Ridge addresses the Homeland Security Tech Expo at the Armory in Washington, D.C., in September 2002. Congress later approved President Bush's plan for a cabinet-level Department of Homeland Security to fight terrorism. AP/WIDE WORLD PHOTOS.

Crisis relegated to history and a new era of U.S.-Soviet détente emerging, use of these measures declined.

The end of the Cold War brought with it new dangers. The enemy was no longer the Soviet Union, a superpower with fairly predictable aims not entirely different from those of the United States. Instead, America faced terrorists whose motives were based upon political and religious zealotry with little regard for international laws, and were therefore more difficult to predict. The reality of the twenty-first century security environment manifested itself on the morning of September 11, 2001.

On October 8, less than four weeks after the attacks, President Bush issued Executive Order (E.O.) 13228 creating the Office of Homeland Security, along with the Homeland Security Council (whose members included the President, Vice President, and several Cabinet-level officials) as

an advisory board. The order gave the office's director the title of Assistant to the President for Homeland Security, nomenclature that harkened to the official title of the National Security Advisor—thus highlighting the importance of the homeland security chief.

For the new position, Bush chose former Pennsylvania governor Tom Ridge, who was approved by the Senate in January 2003. Meanwhile, in November 2002, Congress passed the Homeland Security Act, legislation creating a permanent Cabinet-level department. On January 24, 2003, DHS began operation at its new headquarters at a former U.S. Navy facility, the Nebraska Avenue Center in Washington, D.C. Most agencies scheduled for transfer to the new department were officially moved in a special March 1, 2003, ceremony attended by the President.



In his initial proposal for the creation of DHS, President Bush noted that at that time, there were some 100 government agencies involved in emergency response. DHS would greatly streamline those activities; but before that could happen, a great deal of restructuring would have to occur. The initial appropriation request from the president to Congress was for nearly \$40 billion, and many pundits judged that with the task before it, the new department would need every penny. The creation of DHS was the most fundamental change in the structure of government since the passage of the National Security Act, which created the Department of Defense in 1947.

DHS was scheduled to absorb 22 agencies from nine different departments (Agriculture, Commerce, Defense, Energy, Health and Human Services, Justice, State, Transportation, and Treasury) and two independent offices (FEMA and the General Services Administration, or GSA). With these would come 170,000 government employees, ranging from the men and women of the Coast Guard and Secret Service, to plant and animal health inspectors and computer security specialists.

## DHS Framework

DHS has a threefold mission: to prevent terrorist attacks within the United States, to reduce America's vulnerability to terrorism, and to minimize the danger from potential attacks and natural disasters. In pursuing this mission, DHS works through its five directorates. In order to create these directorates, DHS established some new offices, but much of its framework came from existing ones, listed by the department from which they came:

**Agriculture:** Animal and Plant Health Inspection Service; Plum Island Animal Disease Center.

**Commerce:** Computer Security Division of the National Institute of Standards & Technology; Critical Infrastructure Assurance Office; National Hazard Information Strategy of the National Oceanic & Atmospheric Administration.

**Defense:** National Bio-Weapons Defense Center; National Communications System.

**Energy:** Environmental Measurements Laboratory; Lawrence Livermore National Laboratory; National Infrastructure Simulation & Analysis Center; National Nuclear Security Administration; Nuclear Incident Response; Oak Ridge National Laboratory; Office of Biological & Environmental Research; Office of Energy Assurance; Office of Security.

**Health and Human Services:** Metropolitan Medical Response System; National Pharmaceutical Stockpile Program; National Disaster Medical System/Office of Emergency Preparedness; Office of Health and Safety Information System.

**Justice:** Domestic Emergency Support Team; Executive Office for Immigration Review; INS; National Infrastructure Protection Center (except for the Computer

Investigations and Operations Section, which would remain with the Federal Bureau of Investigation); National Domestic Preparedness Office; and Office of Domestic Preparedness.

**State:** Visa Services.

**Transportation:** USCG; TSA.

**Treasury:** Federal Law Enforcement Training Center (FLETC); USSS; Customs.

Additionally, DHS incorporated FEMA in its entirety, along with two GSA offices, the Computer Incident Response Center and the Office of Federal Protective Service.

**The directorates.** By far the largest component of DHS is the Directorate of Border and Transportation Security (BTS), which is responsible for maintaining the security of the nation's borders and transportation systems. BTS accounts for about 58% of DHS employees, along with nearly half of its operating budget, and includes what was formerly TSA, Customs, the border security functions of INS, the Animal and Plant Health Inspection Service, and FLETC. Like the other directorates of DHS, it is overseen by an undersecretary of homeland security.

Second in size is the Directorate of Emergency Preparedness and Response (EPR), which includes FEMA and numerous smaller agencies. EPR is charged with ensuring that the nation is prepared for and able to recover from both terrorist attacks and natural disasters. The Directorate of Science and Technology (S&T) is DHS's principal research and development arm. Among the areas of focus for S&T is the range of technology needed to prepare for and respond to terrorist threats involving weapons of mass destruction.

Information Analysis and Infrastructure Protection (IAIP) is the directorate concerned with the nation's critical infrastructure, particularly the computer systems that serve as the brain center for a modern industrialized superpower. IAIP brings together a number of specialists capable of identifying and assessing current and future threats to the homeland. Finally, the smallest and least visible directorate is Management, which is concerned with DHS internal affairs, including budget and personnel issues.

**Independent agencies.** In addition to the directorates, DHS includes a number of agencies that, while in some cases associated with specific directorates, nevertheless have an independent existence. Among these is the Coast Guard, which has a clear function in relation to border security but which, upon declaration of war or specific orders from the president, operates as an element of the Department of Defense. Secret Service is also an independent agency within DHS.

Other independent agencies include ones that did not exist as such prior to the establishment of DHS. These

include the Bureau of Citizenship and Immigration Services, which assists the BTS directorate by easing the transition of immigrants to U.S. citizenship; the Office of State and Local Government Coordination; the Office of Private Sector Liaison, which works to foster dialogue between DHS and the business community; and the Office of Inspector General, an independent body responsible for inspection, auditing, and investigating charges of fraud, abuse, mismanagement, and waste.

**DHS in action.** Americans are likely to be most familiar with the DHS advisory system, whereby colors are equated with levels of threat. Green indicates low threat, and blue a “guarded condition” in which there is a general risk of terrorist attacks.

From the time the system was instituted through the spring of 2003, as the United States waged its military campaign in Iraq, the alert level never dipped below yellow, for “elevated condition,” indicating a significant risk of terrorist attacks. On a few occasions it went above yellow and into orange, indicating a high threat of terrorist attacks. During that period, the threat level did not spike above orange to the most severe of conditions, red, though that color would have been used if the color-coded system had been in place at the time of the September 11 terrorist attacks.

On February 7, 2003, concerns about terrorist threats associated with an Islamic holiday caused a raise of the threat level to orange. Ridge encouraged Americans to stock up on food and water, as well as plastic sheeting and duct tape for sealing doors and windows. Ridge was criticized for what some observers described as scare mongering. On February 27, the threat level indicator again returned to yellow. When Ridge hiked it to orange again on March 18, 2003, at the beginning of the war with Iraq, such specific recommendations were not included with the warning; instead it was simply noted for Americans to be vigilant for multiple attempted attacks.

Mayors and governors commented on the fact that, while the DHS called upon cities and states to take extra preparedness measures, it did not provide adequate additional federal funding for such measures. In early April 2003, DHS announced that seven major cities would receive a total of \$100 million to increase anti-terror security efforts.

## ■ FURTHER READING:

### PERIODICALS:

Houston, Betsy. “Science and Technology Is Prominent in the Department of Homeland Security.” *JOM* 55, no. 1 (January 2003): 9.

Hughes, David. “Homeland Security Dept.: So Many Details, So Little Time.” *Aviation Week & Space Technology* 157, no. 23 (December 2, 2002): 71.

———. “Homeland Security Dept.: Is \$36.2 Billion Enough?” *Aviation Week & Space Technology* 158, no. 7 (February 17, 2003): 57–58.

Huleatt, Richard S. “Computer Supersnoop: The New Department of Homeland Security.” *Information Intelligence Online Newsletter* 23, no. 12 (December 2002): 2–4.

Inchniowski, Tom. “Ridge Will Face Big Challenges as Homeland Security Leader.” *ENR* 250, no. 3 (January 27, 2003): 9.

Miller, Bill. “National Alert System Defines Five Shades of Terrorist Threat.” *Washington Post*. (March 13, 2002): A15.

“The New Department of Homeland Security.” *Chemical Engineering Progress* 99, no. 2 (February 2003): 25.

“U.S. Homeland Security: Behind the Curve in Funding and Commitment.” *Aviation Week & Space Technology* 158, no. 9 (March 3, 2003): 66.

Waugh, William L., Jr., and Richard T. Sykes. “Organizing the War on Terrorism.” *Public Administration Review* 62, special issue (September 2002): 145–153.

### ELECTRONIC:

The American Civil Defense Association. <<http://www.tacda.org/>> (April 11, 2003).

Department of Homeland Security Reorganization. C-SPAN. <<http://www.c-span.org/homelandsecurity/chart.asp>> (April 11, 2003).

U.S. Department of Homeland Security. <<http://www.dhs.gov/dhspublic/>> (April 10, 2003).

### SEE ALSO

*Air Marshals, United States*

*Aviation Security Screeners, United States*

*Bush Administration (2001–), United States National Security Policy*

*Civil Aviation Security, United States*

*Coast Guard (USCG), United States*

*Communications System, United States National*

*Critical Infrastructure Assurance Office (CIAO), United States*

*DOE (United States Department of Energy)*

*Domestic Emergency Support Team, United States*

*Domestic Preparedness Office (NDPO), United States National*

*Federal Protective Service, United States*

*FEMA (United States Federal Emergency Management Agency)*

*General Services Administration, United States*

*Health and Human Services Department, United States*

*Infrastructure Protection Center (NIPC), United States National*

*INS (United States Immigration and Naturalization Service)*

*Law Enforcement Training Center (FLETC), United States Federal*

*Lawrence Livermore National Laboratory (LLNL)*

*NNSA (United States National Nuclear Security Administration)*

*NOAA (National Oceanic & Atmospheric Administration)*

*NSC (National Security Council)*

*NIST Computer Security Division, United States*

*Oak Ridge National Laboratory (ORNL)*

*Plum Island Animal Disease Center*

*Secret Service, United States*

*September 11 Terrorist Attacks on the United States*

*Transportation Department, United States*

## HUMINT (Human Intelligence)

Human intelligence, or HUMINT, is the gathering of information through human contact. It is, along with signals intelligence and imagery intelligence (SIGINT and IMINT respectively), one of the three traditional means of intelligence gathering. After the September 11, 2001, terrorist attacks, many observers in the United States decried previous cutbacks in HUMINT that had helped create an environment in which U.S. intelligence was largely unaware of the impending attacks.

**The value of HUMINT.** Whereas SIGINT, IMINT, and non-traditional measurement and signature intelligence (MASINT) are high-tech enterprises, HUMINT is decidedly low-tech. It is a matter, ultimately, of personal interaction, and practitioners of HUMINT are “spies” in the purest sense of the word. The more closely an operative functions in the community, the more his or her information comes from word of mouth, and the more he or she is practicing true HUMINT.

Simple though it may seem in comparison to the sophisticated electronic systems used in the other intelligence-gathering fields, HUMINT is a difficult method that requires precision. Humans are a far more difficult source from which to coax information than are electronic listening devices or cameras. Yet, the information that can come from human sources can be the most useful and up-to-date.

**A hypothetical infiltrator.** Terrorist groups may train in open-air camps whose activities are visible by satellite, but their most important work takes place beyond the reach of satellite photographic equipment. The visual and electronic evidence obtained from the Afghan training camps of the al-Qaeda terror network—the widely aired videotapes of training activities and speeches by leader Osama bin Laden—offered little in the way of concrete clues as to the group’s plans for the devastation of September 11, 2001. Such information would likely have come only by close contact with al-Qaeda operatives on the part of personnel in contact with U.S. authorities.

Most likely, that undercover individual would have been an Arab national. Even though al-Qaeda and their Taliban hosts drew recruits from all over the world, including the United States, even an American of Arab descent would have most likely been under so much scrutiny that his job would have been impossible. Even if the United States had contact with an undercover operative in al-Qaeda circles prior to September 11, that person would probably have come from the same circles as other al-Qaeda members—a world of religious fundamentalists, terrorists, opium smugglers, and arms dealers. In other words, anyone the United States worked with in that

situation was likely to be what most Americans would judge an unsavory character.

An example of such a figure is Ali Mohamed, a former Egyptian army officer who joined the U.S. Army in the 1980s, and trained U.S. Special Forces at Fort Bragg, North Carolina, on Islamic terrorism. Mohamed also served in an undercover capacity, infiltrating the al-Kifah Refugee Center in Brooklyn, New York, where he associated with terrorists. Mohamed later switched alliances, joining Osama bin Laden. Captured and arrested by U.S. authorities, Mohamed told them about al-Qaeda’s plans to bomb two U.S. embassies in Africa—but he only divulged this information in 1999, a year after the bombings occurred.

Disgust with figures such as Ali Mohamed had led the administration of President William J. Clinton to adopt rules of human intelligence that many later blamed for the breaches that made attacks such as those of September 11, 2001, possible. On the heels of revelations that agents of the Central Intelligence Agency (CIA) in Guatemala had committed human rights violations, CIA general counsel Jeffrey H. Smith in 1995 drew up a set of guidelines intended to rid the agency of its association with disreputable characters. The rules prohibited the hiring of agents with records of human-rights violations, barred agents from posing as priests or journalists, and required local CIA recruiters to divulge the identities of recruits to agency headquarters.

**Unintended consequences.** Well-meaning though they may have been, these guidelines further eroded the intelligence-gathering capabilities of an agency whose roster of spies had already been badly reduced two decades earlier by the purges that followed the Church Committee hearings of the mid-1970s. The Iran-Contra scandal of the 1980s had further eroded support for CIA dealings with questionable figures overseas. In subsequent years, the agency had largely sought its intelligence as much as possible through photographic or electronic means.

### ■ FURTHER READING:

#### PERIODICALS:

Fialka, John J. “Aftermath of Terror: Rules for Hiring Agents Are Criticized as Hampering Spy Agencies’ Recruiting.” *Wall Street Journal*. (September 13, 2001): A13.

Jones, Jerry W. “CI and HUMINT or HUMINT and CI or CI/ HUMINT or TAC HUMINT (Confusing, Isn’t It?)” *Military Intelligence Professional Bulletin* 28, no. 2 (April-June 2002): 28–33.

Thomas, Evan. “The Road to September 11.” *Newsweek*. (October 1, 2001): 38–49.

#### SEE ALSO

*Church Committee*  
*CIA, Formation and History*  
*Iran-Contra Affair*  
*Measurement and Signatures Intelligence (MASINT)*

*NIMA (National Imagery and Mapping Agency)  
September 11 Terrorist Attacks on the United States  
SIGINT (Signals Intelligence)*

## Hungary, Intelligence and Security

Part of the Empire of Austria-Hungary preceding World War I, Hungary gained its independence following the collapse of the imperial government in 1918. After World War II, the nation fell under the Soviet sphere of influence as a reluctant satellite nation. The Hungarian government endeavored to dissolve their participation in the Warsaw Pact and break ties with the Soviet Union in 1956. The action was met with Soviet military intervention in the region, and the establishment of a Soviet-influenced government.

During the Cold War, the Hungarian government maintained secret police forces and used intelligence services to conduct political espionage. Like other Soviet satellites, Hungary maintained a censorship state, but media and political controls were less strict than in many other communist nations. During the *détente* years of the 1980s, Hungary began to ease communist regulations, embarking on a program of democratic reforms before most other Warsaw Pact nations. With the collapse of the Soviet Union in 1991, Hungary expedited its ambitious reform plan. One of the first government functionaries to be reformed in post-communist Hungary was the nation's intelligence community.

The primary civilian intelligence organization in Hungary is the National Security Office (NBH). The NBH coordinated most intelligence operations in Hungary, including the gathering and processing of both domestic and foreign intelligence information. The NBH works closely with the National Security Services (NBSzSz) to protect national interests within Hungary's borders, and provide security services for Hungarian government personnel and diplomats at home and abroad. Civilian intelligence has recently focused on the identification and eradication of organized crime syndicates. Political espionage is expressly forbidden, and actions of security forces, including national police, are subject to government review as means of restoring citizen trust in national intelligence and security forces.

In addition to civilian organizations, Hungary maintains military intelligence forces, such as the Military Security Agency (KBH) and the Military Detection Agency (KFH). Though the daily operations of these agencies are classified, the mission of Hungarian military intelligence is identification and neutralization of foreign threats to national security. Military intelligence also conducts anti-terrorism and counterintelligence operations.

Hungary joined the North Atlantic Treaty Organization (NATO) in 1999. The country has petitioned to join the European Union (EU). Having already participated in European anti-terrorism, non-proliferation, and joint-intelligence operations, the Hungarian intelligence community continues to increase its technological and operational capabilities to better aid international, cooperative intelligence efforts.

### ■ FURTHER READING:

#### ELECTRONIC:

Central Intelligence Agency. The World Factbook, 2002. "Hungary." <<http://www.cia.gov/cia/publications/factbook/geos/hu.html>> (March 30, 2003).

#### SEE ALSO

*Cold War (1945–1950): The Start of the Atomic Age*  
*Cold War (1950–1972)*  
*Cold War (1972–1989): The Collapse of the Soviet Union*  
*European Union*

## Hydrophones.

SEE *SOSUS (Sound Surveillance System)*.

## Hypersonic Aircraft

A supersonic aircraft flies faster than Mach 1, or the speed of sound, whereas a hypersonic aircraft is a plane capable of flying at Mach 5, or five times the speed of sound. At sea-level atmospheric pressure, with air temperatures of 59°F (15°C), the speed of sound is about 760 miles per hour (1,225 kph). Hypersonic flight has been possible since the late 1950s, but before it can become practical, designers will have to address some of the physical challenges associated with ultra-high-speed flight.

**The X-15.** On October 14, 1947, Major Charles E. "Chuck" Yeager broke the sound barrier in a Bell XS-1 rocket-powered research plane. Five years later, in 1952, officials at the National Advisory Committee for Aeronautics (NACA) set out to develop a craft capable of hypersonic flight. That craft was the X-15, designed by North American Aviation. The X-15 debuted on October 15, 1958, and between June 8, 1959, and October 24, 1968, more than a dozen pilots in three X-15s flew 199 missions, successively passing Mach 3 (1960), Mach 4 and 5 (1961), and Mach 6 (1963).

Had the X-15 program continued, it might have provided the model, not only for hypersonic flight on Earth, but also for space flight. However, a number of circumstances brought an end to the program. One was a change

in leadership as NACA, founded in 1917, gave way in 1958 to the National Aeronautics and Space Administration (NASA). Another change was the urgent political goal of beating the Soviets in the space race after the surprise launch of the *Sputnik* satellite in 1958. Desirous of putting the first man on the Moon, U.S. leaders bypassed the X-15 flight model in favor of rockets.

The X-15 was also challenged by the physical constraints of hypersonic flight. On October 3, 1967, pilot Peter Knight reached Mach 6.7, and nearly incinerated the tail of his craft. Six weeks later, on November 15, the in-flight breakup of the third X-15 claimed the life of pilot Mike Adams. The X-15 made its final flight on October 24, 1968.

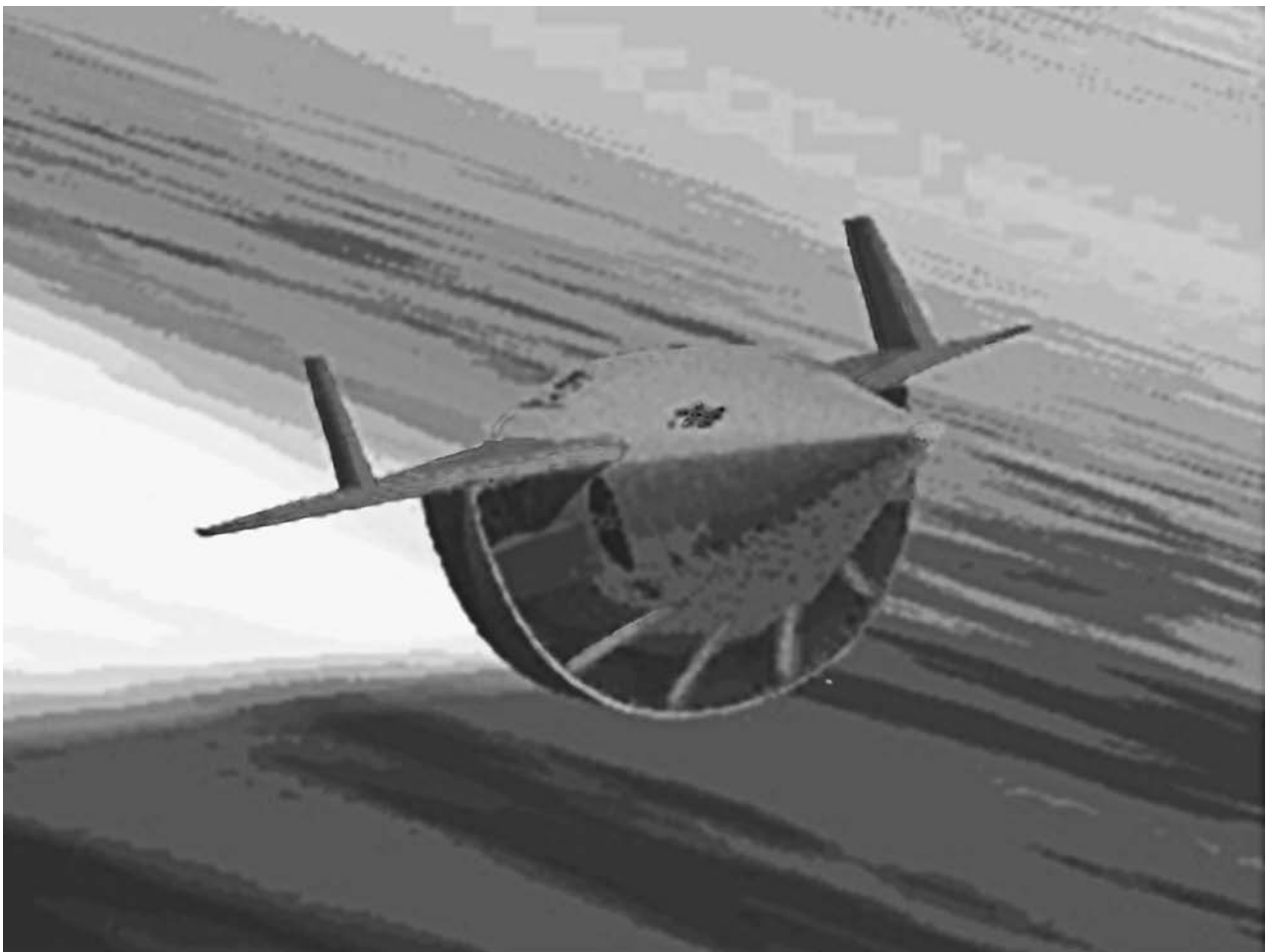
**Other hypersonic studies.** By the time the X-15 ceased operation, the United States had already developed two other extraordinary aircraft, the U2 and the SR-71. The latter, introduced in December 1964, was capable of attaining Mach 3—a speed that, while fast, was not hypersonic. During the early 1990s, the SR-71 was taken off-line

for a few years due to the high cost of keeping it aloft, and this hiatus fanned reports that the U.S. Air Force (USAF) and Department of Defense (DOD) were developing a replacement.

Since 1979, there had been talk of this putative SR-71 successor, identified as “Aurora” by a code name accidentally included in a 1985 Pentagon budget request. However, the USAF and DOD repeatedly denied that they were developing a replacement for the SR-71, which went back into commission in 1995.

Research on hypersonic flight has continued, however. Aerospace engineers have promoted the concept of the HyperSoar hypersonic Global Range Recce/Strike Aircraft, which could attain speeds up to Mach 10 and carry a payload nearly twice as large as that of a subsonic craft. Flying at an altitude of approximately 130,000 feet (39,624 m), it would skip across the top layer of Earth’s atmosphere like a rock skipping across the surface of water.

In June 2001, NASA tested the X-43A, a hypersonic craft with a special engine called a scramjet, which brought together features of both a conventional turbojet and a



An artist’s rendition from the Institute of Future Space Transport at the University of Florida showing one concept for a future space vehicle that would take off and land like an airplane, yet travel at hypersonic speeds. AP/WIDE WORLD PHOTOS.

rocket. It was to be launched by a Pegasus rocket, but unfortunately the rocket failed during the test flight. NASA has continued to work on hypersonic craft, but before such planes can be made operational, engineers will have to develop a means of controlling temperatures so as to keep the craft from bursting into flame as it reenters the atmosphere.

#### ■ FURTHER READING:

##### BOOKS:

- Godwin, Robert. *X-15: The NASA Mission Reports, Incorporating Files from the USAF*. Burlington, Ontario: Apogee Books, 2000.
- Henne, P. A. *Applied Computational Aerodynamics*. Washington, D.C.: American Institute of Aeronautics and Astronautics, 1990.
- Noor, Ahmed Khairy, and Samuel L. Venneri. *Future Aeronautical and Space Systems*. Reston, VA: American Institute of Aeronautics and Astronautics, 1997.

##### PERIODICALS:

- Grier, Peter. "Hypersonic Aircraft Test Fails." *Air Force Magazine* 84, no. 8 (August 2001): 17.
- Leary, Warren E. "Test of Revolutionary Jet Promises to Transform Flight." *New York Times*. (May 22, 2001): F4.

##### ELECTRONIC:

- Aurora/Senior Citizen. Federation of American Scientists. <<http://www.fas.org/irp/mystery/aurora.htm>> (March 4, 2003).
- HyperSoar Hypersonic Global Range Recce/Strike Aircraft. Federation of American Scientists. <<http://www.fas.org/man/dod-101/sys/ac/hypersoar.htm>> (March 4, 2003).
- X-15—Hypersonic Research at the Edge of Space. National Aeronautics and Space Administration. <<http://www.hq.nasa.gov/office/pao/History/x15/cover.html>> (March 4, 2003).

##### SEE ALSO

*Photography, High-Altitude U-2 Spy Plane*



## IBIS (Interagency Border Inspection System)

■ K. LEE LERNER

The Interagency Border Inspection System (IBIS) is a database of names and other identifying information used to deter and apprehend suspects—including suspected terrorists—as they attempt to pass through international border crossing checkpoints.

IBIS provides a rapid means to link names with other identifying information such as passport or credit card numbers. IBIS data is intended for easy crosschecking with other databases such as the FBI's National Crime Information Center (NCIC) database and state-level National Law Enforcement Telecommunications Systems (NLETS) databases.

The IBIS database is also used by more than twenty federal investigative agencies and, following the terrorist attacks on the United States in September 2001, elements of IBIS name-recognition technology are finding increased usage by the FAA and private security companies (principally companies serving airlines and insurance agencies) wishing to identify suspected terrorists. For example, all airlines operating within United States airspace must cross-check passenger and crew lists against IBIS.

As of March 1, 2003, the newly created United States Department of Homeland Security (DHS) absorbed the former Immigration and Naturalization Service (INS). All INS border patrol agents and investigators—along with agents from the U.S. Customs Service and the Transportation Security Administration—were placed under the direction of the DHS Directorate of Border and Transportation Security (BTS). Responsibility for U.S. border security and the enforcement of immigration laws was transferred to BTS.

BTS is scheduled to incorporate the United States Customs Service (previously part of the Department of Treasury), the enforcement division of the Immigration and Naturalization Service (previously part of the Department of Justice), the Animal and Plant Health Inspection Service (previously part of the Department of Agriculture), the Federal Law Enforcement Training Center (previously part of the Department of Treasury), Transportation Security Administration (previously part of the Department of Transportation) and the Federal Protective Service (previously part of the General Services Administration).

Former INS immigration service functions are scheduled to be placed under the direction of the DHS Bureau of Citizenship and Immigration Services. Under the reorganization the INS and other absorbed agencies will formally cease to exist on the date the last of their functions are transferred.

Although the IBIS database is scheduled to continue, in an effort to facilitate border security, BTS plans call for higher levels of coordination between formerly separate agencies and databases. As of April 2003, the specific coordination and future of the IBIS program was uncertain with regard to name changes, database custody, and policy changes.

Prior to integration of INS and Customs service functions into DHS, IBIS was used and maintained principally by those two agencies. Other United States law enforcement and regulatory bodies that utilize IBIS data and technology include the CIA, NSA, FBI, Secret Service, and Coast Guard. International agencies such as Interpol also contribute to and use the IBIS database. Regular updates to lists of names of persons prohibited from entering the United States, criminal suspects, or individuals sought for questioning are provided from a global network of Consular Officers at U.S. embassies and consulates managed by the Department of State.

In addition to attempting to identify terrorists, IBIS is also a key component in attempts by the DEA to deter drug trafficking and ATF attempts to regulate arms shipments. A number of other agencies such as the Internal Revenue



An electronics technician for the U.S. Border Patrol uses a crank to manually turn two surveillance cameras, a thermo imager, right, and a daytime camera, left. AP/WIDE WORLD PHOTOS.

Service (IRS) and Animal Plant Health Inspection Service utilize IBIS to identify individuals suspected of offenses within their respective agency jurisdictions. IBIS is also designed to facilitate identification of vehicles, aircraft, and vessels.

Proponents of the IBIS system argue that the system allows the majority of individuals seeking to cross the border for legitimate purposes to do so in a rapid, uncomplicated manner. Rather than subjecting every individual to what would be a lengthy wait while lists of names from various agencies are checked, IBIS permits a simpler, quicker, and more secure clearance procedure.

In an effort to enhance accuracy, IBIS technology incorporates language analysis software (e.g., name recognition software) and specialized search tools. One goal of name recognition software is to provide a mechanism to correct faulty transliteration of names (e.g. the erroneous translation of an Arabic name into English). Errors common to transliteration—especially oral to written transliterations—include faulty phonetic assignment of letters to unfamiliar ethnic sounds, faulty fusion of syllables (e.g., a fusion of parts of a name such as a given name

with a family name), and faulty assignment of parts of names to specified fields in the input sequence of analysis programs. For example, in some European based languages “van” or “von” is most often a surname prefix but in some Asiatic languages “Van” is most often a surname. Some Arabic names, for example, may be commonly translated into more than thirty different English spellings or variations from the single form found in Arabic.

In standard database searches, if a name entered does not match the spelling or form of a name originally entered in a database, matching the names may be impossible. Standard database search techniques such as key-searches that attempt to match character strings (e.g., specific combinations of letters) often provide erroneous results based upon input errors that occur either during the checking procedure or when a name was originally loaded into the database. More complex search protocols utilize so-called fuzzy logic subroutines that look for similarities and patterns in character strings while allowing for some degree of variation. Fuzzy logic based database search programs allow search protocols to check for common errors, and provide enhanced accuracy to search routines.

The great number of languages and ethnic variations of spellings, however, requires specialized name recognition software. As of 2003, a company under contract to the U.S. government, Virginia based Language Analysis Systems, was developing programs with search components designed to facilitate the identification of the cultural origins of names and terms. Other techniques include protocols that analyze data for specific errors. Other companies have developed programs that apply multiple prefixes and suffixes to input names, use multiple phonetic spellings, translate spellings into various foreign alphabets, and employ result-ranking schemes to enhance search results.

Such name recognition software will play a critical role in linking often dissimilar databases maintained by separate agencies and such “smart” search protocols will be essential in achieving efficiency and accuracy in the new Department of Homeland Security. For example, IBIS combined with the INS Advance Passenger Information System (APIS), allows immigration and customs inspectors to use a single input screen to make a joint search. Other systems targeted for database interface include the FAA Computer Assisted Passenger Screening System (CAPS).

#### ■ FURTHER READING :

##### ELECTRONIC:

Bureau of Citizenship and Immigration Services. INSPASS. March 1, 2003. <<http://www.immigration.gov/graphics/howdoi/inspassloc.htm>> (April 14, 2003).

Department of Homeland Security. April 2, 2003. <<http://www.dhs.gov/dhspublic/index.jsp>> (April 11, 2003).



United States Department of Homeland Security. Bureau of Citizenship and Immigration Services, PORTPASS. March 11, 2003. <<http://www.immigration.gov/graphics/howdoi/portpass.htm>> (April 9, 2003).

United States Department of Homeland Security. Immigration Information, INSPASS. March 4, 2003. <<http://www.immigration.gov/graphics/shared/howdoi/inspass.htm>> (April 9, 2003).

#### SEE ALSO

*APIS (Advance Passenger Information System)*  
*IDENT (Automated Biometric Identification System)*  
*INSPASS (Immigration and Naturalization Service Passenger Accelerated Service System)*  
*NAILS (National Automated Immigration Lookout System)*  
*PORTPASS (Port Passenger Accelerated Service System)*  
*SENTRI (Secure Electronic Network for Travelers' Rapid Inspection)*

---

## IDENT (Automated Biometric Identification System)

---

The Automated Biometric Identification System (IDENT) is a database system using automated fingerprint identification systems (AFIS) technology as part of programs supervised by the U.S. Department of Homeland Security that intend to thwart illegal entry into the United States by criminal aliens.

IDENT was implemented on a trial basis in 1994 and put into wide use by 1998. In August 1998, INS IDENT managers established standardized policies on the use of IDENT but for financial reasons decided not to include historical data in the IDENT database. Accordingly, IDENT queries were limited to returns of data acquired since IDENT implementation. By 1999, approximately 1.8 million biometrics were keyed into the IDENT "recidivist" (repeat offender) database.

The IDENT system biometrics includes photos and the two index finger fingerprints (entered via a portable TouchView fingerprint reader) of individuals previously apprehended by border and immigration agents. That data is augmented by available data on the individual's criminal history. With this data IDENT provides access to both a recidivist database and a "lookout" database for criminal offenders.

IDENT fingerprint searches of the two databases normally takes only a few minutes. IDENT fingerprint matching is based upon a numerical score derived from degrees of relationship in standard fingerprint characteristics. An IDENT terminal then provides agents with photographs and fingerprint displays of individuals under examination alongside photographs and fingerprints of potential

matches. This final visual matching is key because, especially under field conditions, fingerprint analysis is often hampered by dirt on the alien's fingers or the scanner.

Records are ultimately linked to a unique fingerprint identification number (FIN) for each alien. The IDENT fingerprinting technology does not require ink, but uses a machine that scans and digitizes prints before transferring them to a standard ten-print card and storing them in the electronic database.

Use of the IDENT system is critical because studies have shown that apprehended illegal aliens often attempt to falsify their identity by providing a fictitious name and/or a birthdate. As of March 2003, the IDENT database contained records on more than 400,000 aliens who had a history of attempted illegal entry and a criminal history that precluded their entry into the U.S. Prior to DHS reorganization, INS and Border Patrol agents had detained more than 75,000 individuals based on IDENT data.

The IDENT system can also provide basic identification information that allows access to several other security and law enforcement databases including, but not limited to, the Central Index System (CIS), National Automated Immigration Lookout System II (NAILS), Deportable Alien Control System (DACS), National Crime Information Center (NCIC) database, and the Treasury Enforcement Communication System (TECS). Under pending security proposals the IDENT database and system may be fused with the Integrated Automated Fingerprint Identification System (IAFIS) used by the FBI.

As of March 1, 2003, the newly created United States Department of Homeland Security (DHS) absorbed the former Immigration and Naturalization Service (INS). All INS border patrol agents and investigators—along with agents from the U.S. Customs Service and Transportation Security Administration—were placed under the direction of the DHS Directorate of Border and Transportation Security (BTS). Responsibility for U.S. border security and the enforcement of immigration laws was transferred to BTS.

BTS is scheduled to incorporate the United States Customs Service (previously part of the Department of Treasury), and the enforcement division of the Immigration and Naturalization Service (previously part of the Department of Justice). Former INS immigration service functions are scheduled to be placed under the direction of the DHS Bureau of Citizenship and Immigration Services. Under the reorganization the INS formally ceases to exist on the date the last of its functions are transferred.

Although the technologies involved in the IDENT entry security program remained stable, in an effort to facilitate border security, BTS plans to establish higher levels of coordination between formerly separate agencies and databases. As of April 2003, the specific coordination and future of the IDENT program was uncertain with regard to name changes, program administration, and policy changes.

## ■ FURTHER READING :

### ELECTRONIC:

Department of Homeland Security. April 2, 2003. <<http://www.dhs.gov/dhspublic/index.jsp>> (April 11, 2003).

Department of Homeland Security, Bureau of Citizenship and Immigration Services. Law Enforcement: The National Border Patrol Strategy. <<http://www.immigration.gov/graphics/publicaffairs/statements/igstate.htm>> (April 12, 2003).

### SEE ALSO

*APIS (Advance Passenger Information System)*

*IBIS (Interagency Border Inspection System)*

*INSPASS (Immigration and Naturalization Service Passenger Accelerated Service System)*

*NAILS (National Automated Immigration Lookout System)*

*PORTPASS (Port Passenger Accelerated Service System)*

*SENTRI (Secure Electronic Network for Travelers' Rapid Inspection)*

## Identity Theft

■ KELLI A. MILLER

Identity theft is among the fastest growing crimes in America. A thief typically steals someone's identity, opens checking and credit card accounts in that person's name, then goes on a spending spree. The rate of identity theft or identity fraud had so escalated in the late 1990s that the Social Security Administration declared it a national crisis.

Identity theft is the most popular—and most profitable—form of consumer fraud. It encompasses all types of crime in which someone illegally obtains and fraudulently uses another person's confidential information, most often for financial gain. A person's Social Security number is valuable to an identity thief. Armed with the Social Security number, a criminal can open a bank account or credit card account, apply for a loan, and remove funds from varying financial accounts. In some cases, criminals have assumed the victim's identity altogether, amassing debt and committing crimes that become a part of the victim's criminal record.

**The identity trail.** Advanced computer and telecommunication technologies have armed thieves with new ways to obtain large amounts of personal data from afar. Hackers can spy on e-mail and Internet users, silently stealing passwords or banking information. Old-fashioned concepts such as "dumpster diving" still prevail. Thieves sort through garbage for telltale signs of identity such as



Associated Press reporter Nedra Pickler displays the unauthorized credit card bills charged to her name in 2002 after she became the victim of identity theft, a growing crime. In a matter of a week, thieves charged \$30,000 worth of merchandise on credit cards obtained using her identity.

AP/WIDE WORLD PHOTOS.

cleared checks, bank statements, even junk mail, such as "preapproved" credit cards.

Other criminal tactics include "shoulder surfing" and "skimming." A "shoulder surfing" criminal spies on someone as they type in a Pin number or password on an automatic teller machine (ATM). "Skimming," one of the newest schemes, occurs when a cashier receives a credit card for a purchase, then unknown to the victim, swipes it through a portable device that records the card information.

Consumer advocates estimate that 750,000 people will become victims of identity fraud every year. The statistic is a startling difference from numbers logged just a decade ago. In 1992, the credit reporting agency TransUnion logged about 35,000 identity theft complaints. A decade later, the company received more than a million calls.

Measures can be taken to minimize the risk of identity theft. Security experts recommend carrying a limited number of ID cards and credit cards, signing all new credit cards immediately with permanent ink, steering clear from unsecured Internet sites, and never writing a PIN, password, or Social Security number on credit cards or in briefcases or wallets. Cashiers should be observed as they process an order and personal or account information should not be revealed to anyone without first verifying their identity. Other tips include creating passwords that are not obvious (i.e., do not use birth dates) and checking credit reports periodically for accuracy.

**Identity theft affidavit.** In many cases, the victim may not realize their identity has been stolen until a negative situation arises. When the crime is finally discovered, the victim must provide proof that they did not create the debt themselves. This involves a laborious process of contacting each and every company where accounts were fraudulently opened. Persons whose identities have been stolen can spend months, even years, remedying the problem. To reduce the burden, the government established the ID Theft Affidavit, a single form that alerts all participating companies about the crime. A number of financial organizations, including the top three credit reporting agencies, endorse the ID Theft Affidavit.

According to the U.S. Federal Trade Commission (FTC) and U.S. General Accounting Office (GAO), the average victim spends anywhere from \$1,000 to over \$10,000 per incident of identity theft or fraud to reclaim and re-establish identity and credit. Victims of identity fraud should notify all three national credit reporting agencies (Equifax, Experian, TransUnion) immediately and request that their files be flagged with a fraud alert. The crime should also be reported to the police and the FTC, and in some cases, the Social Security Administration, Department of Motor Vehicles, and the U.S. Post Office.

**Identity Theft and Assumption Deterrence Act.** The threat to privacy has prompted a number of new laws governing fraud. In 1998, Congress passed the Identity Theft and Assumption Deterrence Act. The legislation created a new offense of identity theft, making it a separate crime against the person whose identity was stolen. Prior to this legislation, identity theft was considered a crime only against the company the victim defrauded. Under the Federal identity theft act, it is a crime for any person to “knowingly transfer[ring] or use[ing], without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.” Violators face a maximum term of 15 years in prison, a fine, and criminal forfeiture of any personal property used or intended to be used to commit the offense.

ID thieves are often charged with other violations, including credit card fraud, computer fraud, and mail

fraud. These felonies can carry substantial penalties and up to 30 years’ imprisonment. The Federal Bureau of Investigation (FBI), the United States Secret Service, and the United States Postal Inspection Service help prosecute identity theft cases. Many states have also enacted legislation regarding identity theft. Arizona led the way with a specific identity theft statute passed in 1996. As the crime’s serious threat became evident, more states followed suit. In 1999, 22 states passed identity theft legislation. According to a GAO 2002 report, identity theft can be a felony offense in 45 of the 49 states that have laws to address the problem. Two years after the passage of the federal identity theft act, the Justice Department testified that it had used the statute in 92 cases, according to a GAO report.

The Identity Theft and Assumption Deterrence Act required the FTC to “log and acknowledge the receipt of complaints by individuals who certify that they have a reasonable belief” that someone stole their identity. The act enabled the creation of the Identity Theft Data Clearinghouse, a federal database for tracking complaints. Consumers call a toll-free hotline (1-877-ID-THEFT) to enter their complaint, and have the option to do so anonymously. When established in 1999, the FTC logged about 260 calls per week. In December 2001, the hotline was receiving more than 3,000 contacts a week.

Identity fraud complaints and related information are shared electronically between the FTC and other law enforcement agencies nationwide via the Consumer Sentinel Network, a secure, encrypted website. The network was initially set up in 1997 as a way of tracking telemarketing scams. As of May 2002, 46 federal law enforcement agencies and over 18,000 state and local departments had enrolled in the FTC’s Consumer Sentinel Network collaboration. Accessing the Network allows police to analyze identity theft cases and determine if there is a larger pattern of crime. At this time, comprehensive results involving the number of cases prosecuted under the federal identity theft act and state statutes are not available.

#### ■ FURTHER READING :

##### ELECTRONIC:

Federal Trade Commission. “ID Theft: When Bad Things Happen to Good People.” September 2002. <<http://www.ftc.gov/bcp/online/pubs/credit/idtheft.htm#occurs>> (December 11, 2002).

Federal Trade Commission. “Identity Theft.” August 7, 2002. <<http://www.consumer.gov/idtheft/>>(December 01, 2002).

Georgia Stop Identity Theft. “What is Identity Theft?” 2002. <<http://www.stopidentitytheft.org/prevention.html#what>>(December 01, 2002).

ID Theft Resource Center. “ID Theft.” October 28, 2002. <<http://www.idtheftcenter.org/>> (December 01, 2002).

##### SEE ALSO

*Computer Fraud and Abuse Act of 1986*  
*FBI (United States Federal Bureau of Investigation)*  
*Justice Department, United States*

*Postal Security*  
*Postal Service (USPS), United States*  
*Secret Service, United States*

## IFF (Identification Friend or Foe)

Identification friend or foe (IFF) systems are methods of identifying aircraft using electronic means. Applied by both military and civilian entities, IFF—which in its civilian form is more properly known as the air traffic control radar beacon system, or ATCRBS—uses radar to identify aircraft, which are assigned unique identifier codes. There are various modes of operation for IFF, depending on the level of security desired.

**Challenge and response.** In World War II, as radar was emerging, Allied aviators and ground controllers soon became aware of a shortcoming in the existing electronic identification system; radar could only recognize that a plane was in the sky, but could not differentiate friendly planes from those of the Axis. The Germans were the first to develop a crude IFF system, which required pilots to roll their planes in midflight as a means of creating a distinctive radar blip that would identify them as Luftwaffe craft to radar operators. The Allies developed their own active systems: first Mk I in 1940, and later the much more effective Mk III, which greatly enhanced identification technology by adding a separate transmitter that tuned through radar bands even as the receiver in the air did the same. Mk III also was made to respond to as many as six different codes.

From the beginning, IFF was a system of challenge and response, operating on much the same principal as a guard demanding a password before allowing entrance. In the case of IFF, the radar on the ground (the interrogator) transmits on one frequency, and receives a coded signal from the plane's transponder on another frequency. In the United States, these transmissions typically take place at 1030 megahertz (MHz) for challenges, and 1090 MHz for replies.

**Security and modes of operation.** There are several modes of operation, as well as an important submode, relating to levels of security in military IFF operation. Mode 1, for instance, is a nonsecure, low-cost mode used by ships to track aircraft and other ships, while Mode 2 is used by aircraft making carrier-controlled approaches to ships during times of inclement weather.

Commercial aircraft chiefly use Mode 3, the standard system by which they relay positions to ground controllers across the globe. The Federal Aviation Administration

(FAA) requires that all aircraft, military or civilian, that fly at 10,000 feet or higher must be equipped with working IFF transponder systems capable of reporting altitude. To do so requires Mode C, a submode that automatically includes an altitude report.

At the highest security level is Mode 4, the only true IFF system, as opposed to a mere means of differentiating obviously friendly aircraft in order to enable greater control of traffic from the ground. This mode, used on warfighting planes, utilizes sophisticated encryption that includes a long challenge word with a preamble to inform the transponder that it is about to receive a secure message. If the plane's transponder is incapable of deciphering the challenge, it effectively identifies the aircraft as something other than a friend. Key codes are periodically changed and reentered into transponders and interrogators so as to ensure the continued security of codes.

### ■ FURTHER READING:

#### BOOKS:

Launius, Roger D. *Innovation and the Development of Flight*. College Station: Texas A&M University Press, 1999.

Murray, Williamson, and Allan Reed Millett. *Military Innovation in the Interwar Period*. New York: Cambridge University Press, 1996.

Rihaczek, August W., and Stephen J. Hershkowitz. *Theory and Practice of Radar Target Identification*. Boston: Artech House, 2000.

#### ELECTRONIC:

Identification Friend or Foe (IFF) Systems. 551st and 552nd AEW&C Wings, U.S. Air Force. <<http://www.dean-boys.com/extras/iff/iffqa.html>> (March 16, 2003).

#### SEE ALSO

*Codes and Ciphers*  
*Electromagnetic Spectrum*  
*FAA (United States Federal Aviation Administration)*  
*RADAR*  
*Radio, Direction Finding Equipment*

### Imbedding.

SEE *Steganography*.

## IMF (International Monetary Fund)

### ■ STEPHANIE WATSON

The International Monetary Fund (IMF) is an economic organization that promotes financial cooperation, economic stability, and fair trade among its 184 member

nations and provides temporary monetary assistance to countries in need.

In its role as global economic watchdog, the IMF must continually keep an eye out for illegal activities. Following the events of September 11, 2001, that role took on an even greater urgency. Since then, the organization has launched a global effort to combat money laundering and to cut off funding to terrorist groups.

**The need for a new world economic order.** In the early 1940s, the world was still reeling from the financial turmoil of the Great Depression. As markets in the United States and around the world collapsed, countries sought to protect their weakened economies by closing their doors to foreign imports and restricting their citizens from making purchases abroad. The result was catastrophic; world trade nearly ground to a halt. In order to protect the world economy from suffering another similar blow, and to hasten financial recovery among war-torn nations, leaders from forty-five countries came together during the summer of 1944; their historic meeting in Bretton Woods, New Hampshire, established a new international system of economic collaboration called the IMF. The Bretton Woods Conference also launched the IMF's sister organization, the International Bank for Reconstruction and Development (IBRD), or World Bank. On December 27, 1945, representatives from twenty-nine member nations signed the Articles of Agreement, formally bringing the IMF into existence. The initial goals of the organization were to expand international trade, and to protect the stability of international currencies and exchange rates.

**The IMF today.** The IMF currently has three main responsibilities: surveillance, financial assistance, and technical assistance. The IMF keeps a watchful eye over its member nations throughout the year, monitoring each country's exchange rate and economic policies to protect the stability of the world economy. All member countries are entitled to financial assistance to help them recover from an economic crisis or to pay off foreign debt. By 2003, the IMF had about \$88 billion in outstanding loans to eighty-eight nations. Because strategies of the IMF hold that one of the keys to worldwide economic stability is financial self-sufficiency, it has programs in place to teach countries how to plan and implement their own monetary, tax, and exchange rate policies.

With the increasing trend toward globalization (the merging of international markets), the IMF has turned its focus to emerging markets such as Asia and Latin America. By supporting economic growth and fostering the development of stable financial systems in these nations, the IMF hopes to avert an international financial crisis such as the worldwide depression of the late 1920s and 1930s, and to further strengthen the world economy.

Today, the IMF is headquartered in Washington, D.C., and staffed by a team of more than 2,500 people from

nearly 140 countries. At the helm is the Board of Governors, composed of banking leaders and ministers of finance from each member country. The Board of Governors comes together once a year at the IMF-World Bank meeting, but much of the substantial operations are carried out by the twenty-four Executive Directors of the Executive Board. The Managing Director of the IMF serves as Chairman of the Executive Board. Corresponding to each Executive Director is one Governor from the International Monetary and Financial Committee (IMFC). This committee meets twice a year to advise the IMF on issues related to the international monetary system.

A country's voting power is based on the size of its economy and on the amount of the quota (subscription fee) it pays when it joins the IMF, however most decisions are based on a member consensus, rather than on a vote. The United States has the largest quota, contributing nearly 18% of the IMF's total funding.

#### ■ FURTHER READING:

##### BOOKS:

Danaher, Kevin, ed. *Fifty Years is Enough: The Case Against the World Bank and the International Monetary Fund*. Cambridge, MA: South End Press, 1994.

Harper, Richard H.R. *Inside the IMF*. San Diego, CA: Academic Press, 1998.

Stiglitz, Joseph E. *Globalization and its Discontents*. New York: W.W. Norton & Co., 2002.

##### PERIODICALS:

Garritsen De Vries, Margaret. "The IMF Fifty Years Later." *Finance & Development* June 1995: 43—47.

##### ELECTRONIC:

The International Monetary Fund. <<http://www.imf.org>> (January 31, 2003).

##### SEE ALSO

*Federal Reserve System, United States*  
*National Telecommunications Information Administration, and Security for the Radio Frequency Spectrum, United States*  
*Terrorist Organizations, Freezing of Assets*

---

## IMINT (Imagery Intelligence)

---

IMINT, or imagery intelligence, is one of the four major branches of intelligence, along with HUMINT, MASINT, and SIGINT (human, measurement and signatures, and signals intelligence respectively). Formerly known as photographic intelligence, or PHOTINT, IMINT is derived from photography, infrared sensors, synthetic aperture radar, and other forms of imaging technology. It was this wealth of imagery sources and techniques that influenced the

shift in terminology from PHOTINT to IMINT during the 1970s.

Collection platforms for IMINT have ranged from surveillance balloons, employed from the time of the French Revolution onward, to satellites such as those of the KH or KEYHOLE series. In addition to KEYHOLE, CORONA, and other satellite systems employed by U.S. intelligence, there are satellites that are not obviously tasked for intelligence gathering. Aircraft, both manned and unmanned, have long served in the mission of gathering IMINT. These range from the B-17 Flying Fortress of World War II to the U-2, in use since the 1950s, to Pioneer Unmanned Aerial Vehicles used in the Persian Gulf War.

Once gathered, imagery has to be transmitted to processing centers, most of which are in Washington, D.C. Technicians at the National Photographic Interpretation Center (NPIC), the National Imagery and Mapping Agency (NIMA), and other such units are highly skilled at studying photographs taken from high altitudes or from space. From these images, many of which would be extremely difficult for the layperson to interpret in even the most basic sense, imagery technicians can discern information on the movement of troops and materiel, or other enemy activities.

#### ■ FURTHER READING:

##### BOOKS:

*Imagery Intelligence*. Washington, D.C.: Department of the Army, 1996.

Krepon, Michael. *Commercial Observation Satellites and International Security*. New York: St. Martin's, 1990.

Richelson, Jeffrey T. *The U.S. Intelligence Community*, fourth edition. Boulder, CO: Westview Press, 1999.

##### ELECTRONIC:

Imagery Intelligence. Federation of American Scientists. <<http://www.fas.org/irp/imint/>> (April 3, 2003).

##### SEE ALSO

*Balloon Reconnaissance, History*

*Geospatial Imagery*

*NIMA (National Imagery and Mapping Agency)*

*Persian Gulf War*

*Photographic Interpretation Center (NPIC), United States National*

*Photography, High-Altitude*

*Satellites, Spy*

*U-2 Spy Plane*

*Vietnam War*

---

## India, Intelligence and Security

---

Espionage and intelligence appears in the recorded history of the Indus Valley as early as the fifth century.

The modern nation of India gained its independence from Britain in 1947. The withdrawal of the British colonial government left India with little governmental infrastructure, and the nation embarked on an ambitious plan to create a new national government. Indian independence, however, also sparked resistance from ethnic groups on the Indian Subcontinent, such as the large Muslim community. As a result of the developing conflict, India quickly established military and intelligence forces.

India's intelligence community is divided into a traditional structure that separates military and civilian, and foreign and domestic intelligence. Though each agency is charged with its own mission, the government has provided a means to facilitate the sharing of information between members of the intelligence community. The Joint Intelligence Committee (JIC) processes and analyzes data gathered by both civilian and military intelligence agencies and coordinates joint operations. The National Security Council acts as liaison between the government's executive branch and the intelligence services, advising leadership on intelligence and security issues.

The main civilian intelligence agency in India is the Intelligence Bureau (IB). The IB focuses on domestic intelligence, but the exact structure and operations of the agency are largely unknown. Political espionage is illegal in India, and police gathered wiretapping information is inadmissible as evidence in court proceedings. However, the IB conducts regular electronic monitoring of telephone communications, and mail surveillance, despite occasional admonitions from Parliament. The Central Bureau of Investigations handles most criminal investigations, often acting on initial information provided by one of the IB's many departments. Increasing political tensions with neighboring Pakistan altered the focus of IB operations in recent years, with increasing attention paid to the protection and surveillance of national borders.

The Research and Analysis Wing (RAW) is India's primary agency responsible for foreign intelligence. RAW operations are largely focused on espionage against Pakistan. With the addition of both India and Pakistan to the growing cadre of the world's nuclear powers, India's RAW conducts counter-intelligence operations, as well as technological and remote espionage, against Pakistani defense and military interests. The RAW is not subject to Parliamentary review, and its actions are highly secret. The Indian government also used RAW resources to aid predominantly-Hindu Bangladesh's 1971 quest for independence from Muslim Pakistan. Most recently, the RAW aided international antiterrorism efforts by providing the United States and British governments information on the al-Qaeda terrorist network and its strongholds in Pakistan and Afghanistan.

Military intelligence is conducted by the Army Directorate of Military Intelligence. The agency is the weakest of India's intelligence community, but often aids civilian intelligence operations. The Army also maintains the Joint Cipher Bureau, the main code breaking department of Indian intelligence.



Three blindfolded men accused of working for India's intelligence agency and plotting to sabotage Pakistan's 2002 parliamentary elections are presented to the press in Rawalpindi, Pakistan. AP/WIDE WORLD PHOTOS.

To the northwest, the independent Muslim nation of Pakistan claims the Kashmir region of India. The two nations have never resolved the border dispute, and tensions recently reached a climax when both nations declared themselves nuclear powers and began testing weapons of mass destruction. The nuclear programs of India and Pakistan raise interesting questions about the efficacy of current non-proliferation measures and the increasing global prevalence of industrial and scientific espionage. The increasing instability of the region has aroused the concern of the international community and the United Nations Security Council.

#### ■ FURTHER READING :

##### PERIODICALS:

Ramana, M.V., et al. "India, Pakistan, and the Bomb." *Scientific American*. December 2001.

##### SEE ALSO

*Great Game*

## Indonesia, Intelligence and Security

Once the Netherlands's colonial stronghold in the Asian Pacific region, Indonesia gained its independence in 1949. The nation fell under military-influenced authoritarian rule for four decades, but began the transition to demilitarized, popular government in 1985. Since that time, the archipelago nation has strived to flourish despite persistent problems such as growing poverty, tribal and ethnic tensions, territorial disputes, government corruption, and political turmoil. Despite these issues, the government has taken crucial steps to reform and rebuild the nation's intelligence and security communities.

The Indonesian president and the commander of the armed forces administer the Council for the Enforcement of Security and the Law (DPKN). The council is composed of representatives from the nation's government ministries and five main religious councils. DPKN coordinates

intelligence and security force responses to national security threats, utilizing the resources of both military and civilian agencies.

Indonesia has several small civilian intelligence agencies responsible for specific security functions, such as counterintelligence, antiterrorism efforts, government protective services, and media relations. These operational divisions are largely autonomous, but work under the limited direction and coordination of the largest civilian agency, the State Intelligence Coordinating Agency (BAKIN). BAKIN focuses mainly on domestic intelligence information, especially information regarding national defenses.

Another government agency, the Coordinating Agency for National Stability (BAKORSTANAS), combines intelligence and law enforcement activities. The agency is tasked with ferreting out anti-government organizations in Indonesia. However, BAKORSTANAS has few legal limitations on its operations, often detaining and interrogating political dissidents. The agency is under suspicion of human rights violations from several international humanitarian organizations. International criticism prompted the Indonesian government to reform some of the sub-departments of the agency. BAKORSTANAS gained the ability to intervene in social conflicts such as strikes and worker's disputes, but reforms also limited its powers to control action forces without government consent.

Indonesia maintains a three-branch military, including an army, navy, and air force. Each branch of service employs its own strategic intelligence forces within its operations units. BAIS is the nation's main military intelligence agency, and as such oversees and coordinates the efforts of various military intelligence forces. Indonesian military intelligence focuses on foreign intelligence information, especially that garnered from communications surveillance. In recent years, the Indonesian government has made the actions of military intelligence agencies more directly responsible to the DPKN in order to gauge political sentiment within the military and prevent the rise of insurgent groups.

One of the most pressing political and security problems plaguing the Indonesian government was resolved in 2002. In August 1999, the Timor region approved a referendum for independence. After garnering international criticism for their policies and actions regarding Timor, the Indonesian government agreed to the region's appeal for sovereignty. On May 20, 2002, the international community recognized the region, now called East Timor, as an independent state.

Reforms continue to address international concerns of past human rights violations by Indonesia's military and former regime. The nation also embarked on ambitious banking and finance reforms to meet International Monetary Fund (IMF) standards. Despite progress in changing the nation's infrastructure to increase Indonesian participation in the international organizations, political extremist and terrorist groups operating within Indonesia's

national borders undermine the nation's status in the international community.

#### ■ FURTHER READING:

##### ELECTRONIC:

Central Intelligence Agency. CIA World Factbook. <<http://www.cia.gov/cia/publications/factbook/geos/id.html>> (April 18, 2003).

## Industrial Espionage.

SEE *Economic Espionage*.

## Infectious Disease, Threats to Security

#### ■ BRIAN HOYLE

Infectious diseases are those diseases that are caused by microorganisms such as bacteria and viruses, many of which are spread from person to person. An intermittent host, or vector, aids the spread of some infectious diseases. One example is the transmission of the viral agent of Yellow Fever to humans via the bite of a mosquito. Other infectious diseases are spread directly from one person to another via infected body fluids or contaminated droplets in the air, as from a sneeze. Examples include influenza (aerosolized droplets) and hemorrhagic fevers such as Ebola (body fluids).

**The scope of infectious diseases.** Of the estimated 54 million deaths that occurred worldwide in 1998, approximately one-fourth to one-third (i.e., 13.5 to 18 million) were the result of an infectious disease. The bulk of these deaths occurred in the developing world and many involved children.

Infectious diseases have been part of human history for thousands of years. For example, descriptions of a disease with symptoms like those of anthrax, which is caused by the bacterium *Bacillus anthracis*, appear in the Old Testament Book of Exodus; anthrax is also thought to be the "burning wind of plague" mentioned in Homer's epic poem *Iliad*. Another example of an ancient infectious disease is bubonic plague. A huge epidemic of bubonic plague during the Middle Ages was called the Black Death, because of the characteristic skin discoloration produced by the bacterial infection.

The increasing ease of global travel and prevalence of antimicrobial treatments (i.e., antibiotics) in the twentieth





An Israeli Red Star of David worker, right, receives a smallpox vaccination in 2002, after the Israeli government decided to inoculate 15,000 emergency workers who in turn could vaccinate the rest of the population of Israel within four days in the event of a bioterrorist attack. AP/WIDE WORLD PHOTOS.

century produced an increase in the spread of infectious diseases, as well as the emergence of new or newly recognized diseases. One example is Acquired Immuno-deficiency Syndrome (AIDS). Recognized in the 1980s, AIDS is now a world-wide epidemic affecting millions of people. Tuberculosis, which is caused by the bacterium *Mycobacterium tuberculosis* has reemerged as a health threat. More than 30 new infectious diseases have emerged since 1975.

#### Infectious disease and security: Disease as a weapon.

Throughout most of recorded history, the suffering and huge loss of life produced by infectious diseases like anthrax and bubonic plague has mostly been accidental. Nonetheless, biological warfare is also ancient. For example, hundreds of years ago, the bodies of cattle were dumped into wells to poison the drinking water, and the bodies of human victims of anthrax were catapulted into fortified cities to spread the disease to the enemy.

In the twentieth century, the use of infectious disease as a weapon and security threat became an accepted strategy of war. Anthrax weaponry was researched in

World Wars I and II. During World War II, Britain produced millions of anthrax packages that were planned for air dropping in Germany to infect the population as well as the food chain. The ancient infections of anthrax and plague, along with smallpox, were explored as biological weapons by the former Soviet Union. Soviet scientists considered these microbes as strategic weapons, potentially capable of destroying entire populations.

In the last few decades of the twentieth century, the use of infectious disease became part of the arsenal of terrorist organizations. For example the Japanese cult Aum Shinrikyo, which released poison gas into the Tokyo subway system in 1995, killing 12 people and hospitalizing thousands, was also developing weapons to disperse the Ebola virus and anthrax spores.

The mass illness and death caused by the deliberate release of an infectious microorganism is a threat to the security of a country. The microorganisms can be easily disguised and transported virtually anywhere people can travel. As well, various microbes can be spread by insects, the wind, and in water. Thus, traditional security measures that have secured borders from other threats are ineffective against the deliberate use of microorganisms.

The consequences of the deliberate use of infectious agents are potentially catastrophic. For example, it has been estimated that the release of 100 kilograms of powdered anthrax upwind of a city as compact and populated as Washington, D.C. could kill up to 300,000 people and cripple the operation of the city.

Part of the appeal of the use of infectious disease as a weapon is the economic hardship that can be caused. A 1997 report from the United States Centers for Disease Control and Prevention conservatively estimated that the costs of dealing with the aftermath of an anthrax outbreak in a major urban center would be approximately \$26.2 billion (U.S.) per 100,000 people. In a city such as New York, the tally could be in the thousands of billions of dollars. Several such attacks might bankrupt a country.

This economic drain would be on top of the already excessive economic burden that countries face in dealing with natural disease outbreaks. The cost of dealing with a long-lasting disease such as tuberculosis can be thousands of dollars per person. And, hospitalization is frequently required, which strains a nation's health care infrastructure.

**Infectious disease and security: The spread of infection.** The main security threat from infectious diseases remains the spread of a disease through the population. For example, in 2000, 1,128 cases of malaria were imported into the United Kingdom by arriving travelers. Once in a country, an infection can spread rapidly. This has happened in the United States and Canada with West Nile fever. From a handful of cases in New York City in 1999, the virus has spread to most of the continental U.S. and Canada, and has sickened or killed thousands of people.

This ease of disease spread has produced unexpected outbreaks of disease all over the world. A few examples include legionellosis and leptospirosis in Australia, yellow fever and Creutzfeldt-Jacob disease in Europe, and West Nile fever, hantavirus pulmonary syndrome, cryptococcosis and *Escherichia coli* O157:H7 in North America.

Another aspect of infectious disease that is a threat to security is the emergence of bacteria that have acquired resistance to the treatments used against them. A well-known example is the increasing resistance of bacteria to antibiotics. The microorganisms that cause infectious diseases such as AIDS, tuberculosis, malaria, and hospital-acquired infections are becoming more prevalent.

The development of resistance is a natural process, as a microbe seeks to adapt to the stress imposed by the antimicrobial agent. However, the refinement of genetic engineering technologies has made possible the tailoring of bacteria and viruses so as to be more lethal.

**Current security issues.** In June 1996, U.S. President Bill Clinton initiated a process to develop a national policy

concerning infectious diseases. A part of this policy concerned the influence of infectious diseases on the country's internal and international security. A report issued in 2000 by the National Security Council warned that the economic downturn and political destabilization caused by epidemics of infectious disease, primarily in underdeveloped countries, could constitute a security threat to the United States in the twenty-first century. In the underdeveloped world, the majority of deaths due to infectious diseases involve children. Thus, the next generation of some countries has been decimated. U.S. reliance on the natural resources of the affected countries, and the hostility towards the West that could develop in the underdeveloped world, could put the U.S. and other developed nations at risk.

In 2002, the principal government-sponsored security threat for biological weapon use came from Iraq. The government of Saddam Hussein had previously sanctioned a biological weapons development program. The Iraqi government acknowledged past production and testing of thousands of liters of anthrax-contaminated material for use as weapons. This threat was one of the primary reasons for the 2003 war that toppled the Hussein government.

As more states and groups develop the capacity for biological warfare or terrorism, the security threat against military and civilian personnel grows. For example, in the aftermath of the September 11, 2001 terrorist attacks in the U.S., several incidents of deliberate dispersal of anthrax bacterial spores occurred. These incidents highlighted the ease by which the biological agents could be delivered to their target in something as nondescript as a letter.

#### ■ FURTHER READING:

##### BOOKS:

Inglesby, Thomas V. "Bioterrorist Threats: What the Infectious Disease Community Should Know about Anthrax and Plague," in *Emerging Infections* 5. Washington, DC: American Society for Microbiology Press, 2001.

##### PERIODICALS:

Kaufmann, A.F., M.I. Meltzer, and G.P. Schmid. "The Economic Impact of a Bioterrorist Attack: Are Prevention and Postattack Intervention Program Justifiable?" *Emerging Infectious Diseases* no. 3 (1997): 83-94.

##### ELECTRONIC:

Central Intelligence Agency. "The Global Infectious Disease Threat and Its Implications for the United States." January 2000 <<http://www.cia.gov/cia/publications/nie/report/nie99-17d.html>> (22 November 2002).

World Health Organization. "Strengthening Global Preparedness for Defense against Infectious Disease Threats." Statement to the United States Senate Committee on Foreign Relations—Hearing on The Threat of Bioterrorism and the Spread of Infectious Diseases. 5

September 2001 <[http://www.who.int/emc/pdfs/Senate\\_hearing.pdf](http://www.who.int/emc/pdfs/Senate_hearing.pdf)>(24 November 2002).

#### SEE ALSO

*Anthrax, Terrorist Use as a Biological Weapon*  
*USAMRIID (United States Army Medical Research Institute of Infectious Diseases)*

## Infinite Justice, Operation.

SEE *Enduring Freedom, Operation.*

---

## Information Security

---

■ LARRY GILMAN

Information security, often compressed to “infosec,” is the preservation of secrecy and integrity in the storage and transmission of information. Whenever information of any sort is obtained by an unauthorized party, information security has been breached. Breaches of information security can be grouped into five basic classes: (1) interception of messages; (2) theft of stored data; (3) information sabotage (i.e., alteration or destruction of data belonging to another party); (4) spoofing (i.e., using stolen information to pose as somebody else); and (5) denial of service (i.e., deliberate shutdown of cash machines, electric-supply grids, air-traffic control networks, or the like). Individual computer experts (“hackers”), intelligence agencies, criminals, rival businesses, disgruntled employees, and other parties may all seek to breach information security. All these parties, plus law-abiding private individuals who wish to guard their privacy and protect themselves from identity theft, also have an interest in preserving information security.

Messages and secrets have been subject to interception and theft ever since the invention of writing, but the modern situation is especially challenging. Electronic storage, processing, and transmission of information are now ubiquitous in the developed world, creating novel vulnerabilities. People are authorized to withdraw cash or purchase products on the basis of a piece of information (password or credit card number); trade secrets and business plans are electronically transmitted around the globe. In the U.S., over 95% of military and intelligence communications pass through network facilities owned by private carriers (e.g., the telephone system). Private speech may be broadcast locally by a mobile or cellular telephone or transmitted digitally over a network that can be tapped in numerous locations; databases full of confidential data reside in computers that can be accessed, perhaps illegally, by other computers communicating through networks; and so on. Information security—or insecurity—is a pervasive fact of modern life.

Consequently, breaching information security has become a common practice. For example, credit-card fraud costs approximately \$20 per card per year. In 1994, an international criminal group used the Internet to penetrate Citicorp’s computer system and shift \$12 million from legitimate users’ accounts to its own. Two ex-directors of the French intelligence agency DGSE (Direction Generale de la Sécurité Extérieure) have confirmed that one of the agency’s highest priorities is to spy on non-French corporations and business-related government agencies. United States government agencies such as the Office of the U.S. Trade Representative and high-tech companies such as Boeing, General Dynamics, Hughes Aircraft, and others have been specifically targeted by French espionage—and probably also by other organizations that happen to be less frank (or more prudent) in their public statements.

There are many tools for increasing information security, including software that scans for computer viruses or prevents unauthorized intrusions into computer systems from the networks; password systems of all sorts; physical access security for computers, discs, passcards, credit cards, and other objects containing sensitive information; and encryption of messages and of databases. While all these tools are important to the conduct of business by a large business or government department, passwords and encryption are probably the most important.

Passwords have the advantage of being simple to use. They are not, however, capable by themselves of providing a high level security for large numbers of users. First, most users are asked to supply passwords for many different systems: banking, shopping, e-mail, and so forth. This tempts users to choose short passwords (which are easier to remember but also easier to guess, therefore weaker) and to use the same password for more than one system (causing a domino effect if a password is guessed).

Cryptography—the process by which raw message information (*plaintext*) is mapped or *encrypted* to a scrambled form (*ciphertext*) before transmission or storage, then mapped back to its original form again (*decrypted*) when an authorized party wishes to read the plaintext—is arguably the ultimate tool of information security. High-quality cryptographic systems that are breachable (if at all) only by resource-rich groups like the U.S. National Security Agency are widely available to businesses, governments, and private individuals. Appropriate cryptography can virtually guarantee the security of messages in transit and of information in databases; it can also, through “authentication,” act as a super-password system whereby the identity of a would-be user (or information service supplier) can be positively confirmed. Cryptography has the disadvantages of added complexity, higher cost, and system slowdown.

Cryptography is also politically controversial, despite—or rather, because of—its technical power. Governments, corporations, private individuals, and private groups all have both legitimate and, occasionally, illegitimate motives for information security. Law-abiding persons and groups, or those rebelling against repressive laws, wish to

be secure from surveillance by governments; criminals, terrorists, and the like also wish to be secure from surveillance by governments; government agents who are committing crimes wish to avoid public exposure; and so forth. It is generally advantageous to *all* parties, whether their activities are legitimate or illegitimate in whatever sense, to advocate maximum privacy for their own activities; it is generally advantageous to *governments* to advocate, in addition, maximum transparency for everyone else. Thus, for example, the U.S. government has sought (with little success) to prevent the spread of high-quality encryption algorithms, such as Pretty Good Privacy, outside the U.S., and inside the country has sought to establish voluntary compliance with “escrowed” cryptography systems. In such systems a government agency stores copies of cryptographic keys that enable it to decrypt communications between private parties using the system. In theory, these escrowed keys would be released to police or other government agents only when the court system had determined that there was a legitimate law-enforcement or national-security need to do so. Because such systems allow for third-party access to encrypted information by design, they are intrinsically less secure than a non-escrowed cryptography system, and therefore predictably unpopular with the private sector.

#### ■ FURTHER READING:

##### BOOKS:

Dam, Kenneth W., and Herbert S. Lin, eds. *Cryptography's Role in Securing the Information Society*. Washington, DC: National Academy Press, 1996.

Hoffman, Lance J., ed. *Building in Big Brother: The Cryptographic Policy Debate*. New York: Springer-Verlag, 1995.

##### ELECTRONIC:

Information Systems Security Association: The Global Voice of the Information Security Profession. 2003. <<http://www.issa.org/>> (February 21, 2003).

##### SEE ALSO

*Computer Hardware Security*  
*Computer Software Security*  
*DNA sequences, Unique*  
*Encryption of Data*  
*Information Security (OIS), United States Office*  
*Pretty Good Privacy (PGP)*

---

## Information Security (OIS), United States Office of

---

The Office of Information Security (OIS) is a unit within the General Service Administration (GSA) charged with the

protection of computer data for the federal government. It employs a team of skilled technicians and specialists to manage, store, process, and most importantly provide security for electronic information systems. Under the umbrella of the GSA Federal Technology Service (FTS), OIS is part of the critical infrastructure protection system of the federal government.

The mission of OIS is to provide technology security systems to federal agencies to reduce risks and exposure of critical and sensitive information, and to do so in a cost-effective manner. To fulfill this mission, OIS has on staff an experienced group of technical specialists trained in protection and security methods for electronic data. In addition, it is capable of deploying engineers and technicians from the private sector as needed to federal or allied facilities anywhere in the world to meet transmission, storage, and processing requirements.

Among the solutions at the disposal of OIS are firewalls, or systems to prevent unauthorized access of hardware or software to or from a private network. Other techniques and principles applied by OIS include intrusion detection, security planning, risk management, data encryption, contingency planning, configuration management, and network mapping.

In accordance with President Decision Directive (PDD) 63, issued by President William J. Clinton in May 1998, OIS has worked to protect federal critical infrastructure from attacks by computer hackers. In 1999, it began working with firms in the private sector to provide infrastructure security consulting to federal agencies.

Beginning in October 2000, OIS divided its functions between its Information Security Services Center and its new Office of Information Assurance and Critical Infrastructure Protection. FTS took control of the first of these, through which OIS had met customer-service needs with offerings such as the Safeguard Program and the Access Certifications for Electronic Services Program. Meanwhile, the OIS concentrated its efforts in the critical infrastructure protection area, serving the imperatives of PDD-63 by providing cyber attack incident warnings and response services through the Federal Computer Incident Response Capability.

#### ■ FURTHER READING:

##### PERIODICALS:

Frank, Diane. “GSA Preps Security Pacts.” *Federal Computer Week* 13, no. 6 (March 15, 1999): 1.

##### ELECTRONIC:

Office of Information Security. General Service Administration Federal Technology Service. <<http://www.fts.gsa.gov/infosec/>> (March 4, 2003).

##### SEE ALSO

*Computer Hardware Security*  
*Computer Software Security*

---

## Information Warfare

---

■ JUDSON KNIGHT

The term “information warfare” refers not to a single idea or phenomenon, but to a variety of tools and techniques all centered around the concept that military success is as much a matter of information and ideas as of weapons and tactics. According to the National Defense University’s Martin C. Libicki, seven distinct areas of information warfare exist. These include command and control, intelligence-based, electronic, psychological, and economic information warfare, as well as cyberwarfare and computer hacking. Examples of information warfare in practice include a number of techniques applied by the United States in Western Hemisphere conflicts and the Persian Gulf War of 1991, as well as the overall campaign of “shock and awe” waged as part of the 2003 Operation Iraqi Freedom.

### Libicki’s Definition and Critique

According to Libicki, the seven components of information warfare include command-and-control warfare, designed to strike at the enemy’s command systems, leadership, and infrastructure; intelligence-based warfare; electronic warfare, including cryptographic and radio-electronic techniques; psychological warfare, involving the use of information to influence the views of allies, enemies, and neutrals; “hacker warfare,” or attacks on enemy computer systems; economic information warfare, the control of information in pursuit of economic dominance; and cyberwarfare, which Libicki describes as “a grab bag of futuristic scenarios” involving computer technology.

Libicki has cautioned, not only that “information warfare” is not a single, monolithic entity, but that its value in some cases has been overestimated. He has sought to distinguish between historically useful forms of information warfare, and others that he dismisses as “fantastic,” or “involv[ing] assumptions about societies and organizations that are not necessarily true.”

Even though information systems are becoming increasingly more important to defensive forces, Libicki has maintained it is not necessarily the case that attacks on information systems yield increasing returns, the reason being that these systems have increasingly become distributed and compartmentalized. Above all, it is Libicki’s contention that, outside of specific applications such as electronic jamming, information should not be regarded as a medium of warfare to any greater degree than other aspects of combat support such as logistics.

## Shock and Awe, Rapid Dominance, and Decisive Force

Notwithstanding these cautionary statements, the quick U.S. victory in Operation Iraqi Freedom revealed the success of information warfare as articulated by Harlan K. Ullman, James P. Wade, and others in *Shock and Awe: Achieving Rapid Dominance*. The book, published in 1996 by the Center for Advanced Concepts and Technology, provided a strategic blueprint for the methods applied seven years later in Iraq.

“Shock and awe” defines two principal components of combat, “rapid dominance” and “decisive force.” These can be equated to threats and intimidation (rapid dominance), coupled with the ability to back up those threats (decisive force). The analogy is not a perfect one, however, because rapid dominance also involves the use of force, albeit in a more limited and targeted fashion.

The objective of rapid dominance is to control the perceptions, understanding, and even the will of the adversary, whereas that of decisive force is military victory. Rapid dominance uses military force in support of its objective, so as to make the enemy impotent—or convinced that he is impotent, which amounts to much the same thing. Use of military capabilities within the framework of decisive force is more straightforward, and once again supports its objective.

Accordingly, forces employed for rapid dominance may be much smaller than those of the opposition, as long as they possess the advantage in training and technology. In the case of decisive force, the technological edge is likewise critical, but so is sheer volume of numbers. It follows that casualties may be high in the case of decisive force, while they could be relatively low in the realm of rapid dominance. Speed of action, desirable for decisive force, is essential to rapid dominance, whose scope is all-encompassing rather than a matter of one fighting group against another.

### Information Warfare in Action

Long before “shock and awe,” or even more general modern concepts of information warfare, military forces practiced basic principles of psychological warfare. Ancient Biblical texts describe several instances in which the armies of the Israelites used psychological tactics in one form or another against their enemies, including banging loud cymbals and shouting as a means of convincing the inhabitants of their numbers and aggressive intentions.

Assyrian armies employed “shock and awe”-style techniques apparently designed to influence by intimidation as much as by sheer military force. It has been noted by military historians that the Nazis’ blitzkrieg style of warfare—which again was as effective psychologically as it was militarily—was influenced by the Assyrians’ high-speed chariot warfare tactics. The Nazis also seem to



CNN broadcasted this 1998 Defense Department video of an Iraqi radio relay facility moments before its destruction by a 1600-pound laser-guided bomb during airstrikes by U.S. and British forces. AP/WIDE WORLD PHOTOS.

have appropriated aspects of the iconography and military regalia used by the Assyrian empire to impress and psychologically dominate their foes.

Certainly German leaders made use of Roman symbols such as the war eagle, which may have been influenced by Assyrian models. The Romans themselves, of course, were ancient masters at psychological warfare, from their impressive uniforms and the legions' imposing battle standards to the triumphal parades, in which defeated kings and their treasures were paraded through the streets of the capital city.

Aided by propaganda minister Josef Goebbels, as well as architect Albert Speer and others, Adolf Hitler made his forces into an intimidating spectacle for all the senses. Every aspect of Nazi regalia, beginning with the bold red flag and its intimidating black swastika on a white field, was intended to present an image of overwhelming power. The swastika was an ancient Buddhist symbol for life, but when the Nazis adopted it for their own purposes, they made two critical changes. Turning the symbol to the

right, along with a 45-degree shift of its axis, the symbol resembled a wheel rolling forward against all adversaries.

As powerful as the dextrogyrate (rightward-turning) swastika were the uniforms of the German forces, particularly the SS. These have been repeatedly imitated, and even parodied in movies, but they are unparalleled in the care with which they were designed. The black SS uniform, with its black boots, jodhpurs, and swastika armband, could make even a slight, bespectacled figure such as SS director Heinrich Himmler—a chicken farmer before he joined the Nazi regime—appear intimidating. After the war, when the Nazis who had not committed suicide or escaped were placed on trial at the World Court in The Hague, they looked small indeed in civilian clothes, a testament to the terror inspired by their uniforms.

Nazi psychological warfare with visual images also included their wide use of film for propaganda purposes. They even flirted with television, then in its developmental stages. Nor did they ignore the aural sense: for example, they equipped their Stuka dive-bombers with sirens for no

purpose other than to strike fear into their victims. Late in the war, Hitler fired his V2 rockets toward London, and though they had limited success militarily, these too served a strong psychological warfare purpose.

American forces were latecomers to the idea of psychological warfare, though they did wage a number of successful propaganda campaigns in World War II through the use of leaflets and radio broadcasts. Attempts to win “hearts and minds” in the Vietnam War proved much less successful, however, in part because the United States lacked a clear strategic plan in that war.

In contrast to lack of U.S. success in strategic psychological warfare were a number of achievements in tactical psychological operations, or psyops. In the late 1940s, for instance, operatives with knowledge of rural Filipino folklore used sounds and imagery to convince local Philippine communist insurgents that they were being chased by ghosts.

**Operation Just Cause and Commander Solo.** During Operation Just Cause, the campaign against Panama’s General Manuel Noriega in 1989, psychological warfare experts accompanied U.S. Army Rangers on airborne missions. They broadcast U.S. propaganda from loudspeakers, and bombarded the Vatican embassy, where Noriega had taken refuge, with loud rock music.

Aiding U.S. psychological and propaganda techniques is an array of technology, an example of which is the EC-130F aircraft flown on “Commander Solo” missions. These carry equipment for broadcasting on the AM, FM, television, and military communications bands, with missions flying at the highest possible altitude to ensure maximum coverage.

Commander Solo operated in Just Cause, during which it broadcast propaganda against the Noriega regime. During Operation Uphold Democracy in 1994, it was used for radio and television broadcasts to the people of Haiti, and its frequent relays of messages from President Jean-Bertrand Aristide contributed significantly to the orderly transition from military to civilian rule. In 1991, during Operation Desert Storm, or the Persian Gulf War, Commander Solo aircraft deploying from bases in Saudi Arabia and Turkey broadcast a program called *Voice of the Gulf*, along with other programs designed to convince Iraqi soldiers to lay down their arms.

**The Persian Gulf War.** U.S. psyops tactics in the 1991 Persian Gulf War revealed considerable sophistication. While U.S. forces jammed local radio signals, they broadcast on their own channels, and even dropped portable radios into Iraqi units so as to ensure that opposition forces would hear U.S. broadcasts. Members of the 13th Psychological Operations Battalion operated among prisoners of war in camps, playing “good cop” to the “bad cop” of the military police.

Whereas the latter carried weapons and enforced order, psyops personnel presented themselves as the

prisoners’ friends. They provided them with prayer mats and signs indicating the direction of the Moslem holy city of Mecca, and passed out cigarettes, extra food, and candy to those who cooperated. Each night, they showed the prisoners movies for entertainment, but uncooperative detainees were not allowed to attend. Recalled one member of the 13th Psyops, “We had some Iraqi movies that were [made] according to strict Muslim laws, but they didn’t want to see those. They wanted to see *Superman*.”

The Iraqis made their own attempts at psychological warfare in at least one regard. Using a tactic applied by Axis radio broadcaster Tokyo Rose against Allied forces in the Pacific during World War II, and by Hanoi radio against American GIs in Vietnam, they attempted to convince enemy soldiers that their wives and girlfriends were cheating on them back home. One leaflet that was intended to inform the American soldier that his wife was being unfaithful at home referred to a figure the Iraqis apparently mistook for a film star: Bart Simpson, actually a cartoon character.

**Operation Iraqi Freedom.** Both in Operation Desert Storm and Operation Iraqi Freedom 12 years later, U.S. forces made extensive use of propaganda leaflets. In Operation Desert Storm alone, 14 million leaflets were dropped over Iraq. These were designed to be as simple as possible, keeping in mind the fact that many Iraqi soldiers had only enough education to enable them to read the Koran. Therefore, leaflets relied on images such as a picture of Americans making an amphibious landing—a ruse designed to divert Iraqi defenses for an attack that never occurred.

In early March 2003, just before the launch of Operation Iraqi Freedom, coalition aircraft operating from Turkey undertook Operation Northern Watch, in which they dropped leaflets over Kurdish areas in northern Iraq. The leaflet campaign continued and expanded as hostilities began, and forces bombarded Iraq with messages designed to win over the populace, and to convince the Iraqi military that resistance was futile. An example of the latter was a leaflet that stated, “Attention Iraqi air defense. Any hostile action by Iraqi air defenses toward coalition aircraft will be answered by immediate retaliation. Iraqi air defense positions which fire on coalition aircraft or activate air defense radar will be attacked and destroyed.”

Other psychological tactics employed in Operation Iraqi Freedom included announcements by U.S. leadership that Iraqi leaders were prepared to surrender at the outset of the war. Coalition forces used amplified sound to convince Iraqi forces that tanks were operating outside the city of Basra, and continually broadcast to the populace over radio and television.

Coalition aircraft dropped millions of leaflets over Iraq even after the fighting ended, with the purpose of convincing the Iraqi populace that the invaders had come not to conquer, but to turn the country over to its people. The coalition also released a set of playing cards depicting

key personnel from the regime of dictator Saddam Hussein who had yet to be caught or otherwise neutralized. Hussein himself was the ace of spades.

■ FURTHER READING :

BOOKS:

Alexander, John B. *Future War: Non-Lethal Weapons in Twenty-First Century Warfare*. New York: St. Martin's Press, 1999.

Lesser, Ian O. *Countering the New Terrorism*. Santa Monica, CA: RAND, 1999.

Libicki, Martin C. *What Is Information Warfare?* Washington, D.C.: National Defense University, 1995.

Schwartz, Winn. *Information Warfare: Chaos on the Electronic Superhighway*. New York: Thunder's Mouth Press, 1994.

Ullman, Harlan, James P. Wade, et al. *Shock and Awe: Achieving Rapid Dominance*. Washington, D.C.: Center for Advanced Concepts and Technology, 1996.

ELECTRONIC:

Information Warfare and Information Security on the Web. Federation of American Scientists. <<http://www.fas.org/irp/wwwinfo.html>> (April 14, 2003).

The Information Warfare Site. <<http://www.iwar.org.uk/>> (April 14, 2003).

Institute for the Advanced Study of Information Warfare. <<http://www.psycom.net/iwar.1.html>> (April 14, 2003).

SEE ALSO

- Americas, Modern U.S. Security Policy and Interventions FM Transmitters*
- Iraqi Freedom, Operation (2003 War Against Iraq)*
- Persian Gulf War*
- Propaganda, Uses and Psychology*
- Short-Wave Transmitters*
- World War II*

## Infrared Detection Devices

■ LARRY GILMAN

Infrared detection devices are sensors that detect radiation in the infrared portion of the electromagnetic spectrum ( $>10^{12}$  to  $5 \times 10^{14}$  Hz). Often, such devices form the information they gather into visible-light images for the benefit of human users; alternatively, they may communicate directly with an automatic system, such as the guidance system of a missile.

Because all objects above absolute zero emit radiation in the infrared part of the electromagnetic spectrum, infrared detection provides a means of "seeing in the dark"—that is, forming images when light in the visible portion of the spectrum ( $>4.3 \times 10^{14}$  to  $7.5 \times 10^{14}$  Hz) is scarce or absent. Because the warmer an object is, the



A U.S. Navy aviation systems warfare operator searches for and tracks surface contacts using radar and the Infrared Detection System during a flight mission in support of Operation Enduring freedom in October 2001. AP/WIDE WORLD PHOTOS.

more infrared radiation it emits, infrared imaging is also useful for the detection of outstanding heat sources that may be invisible or hard to detect even when there is ample visible light (e.g., exhaust heat from ships, tanks, jets, or rockets). Many devices used by police, security, and military organizations, including user-wearable, gun-mounted, vehicle-mounted, missile-mounted, and orbital systems, exploit some form of infrared detection technology.

**Principles of infrared detection.** Infrared—"below-red"—light consists of electromagnetic radiation that is too low in frequency (i.e., too long in wavelength) to be perceived by the human eye, yet is still too high in frequency to be classed as microwave radio. Infrared (IR) light that is just beyond the human visual limit ( $>1.0 \times 10^{14}$  to  $4.0 \times 10^{14}$  Hz) is termed near IR, while light farther from the visible spectrum is divided into middle IR, far IR, and extreme IR. Military and security systems utilize mostly near IR and a narrow band in the far IR centered on  $3.0 \times 10^{13}$  Hz,



because the Earth's atmosphere happens to be transparent to IR radiation primarily in these two "windows."

All objects above absolute zero glow in the far IR, so no source of illumination is needed to image scenes using such radiation; to image scenes in near IR, illumination from a light-emitting diode or filtered light bulb must be supplied. Near-IR imagers, however, are still cheaper than passive, far-IR imagers.

There are two basic designs for electronic IR imagers. The first is the scanner. In this design, light from a tiny portion of the scene to be imaged is focused by an optical and mechanical system on a small circuit element that is sensitive to photons in the desired IR frequency range. The intensity of the signal from the IR detector element is recorded, then the mechanico-optical system shifts its focus to a different fragment of the scene. The response of the IR detector element is again recorded, the view shifts again, and so forth, systematically covering the scene. Many scene-covering geometries have been employed by scanning imagers; the scanner may record horizontal or vertical lines (rasters), spiral outward from a central point, cover a series of radii, and so on.

The second basic type of IR imaging system is the "starer." Such a system is said to "stare" because its optics do not move like a scanner's, scanning the scene a little bit at a time; instead, they focus the image onto an extended focal plane. Located in this plane is a flat (planar) array of tiny sensors, each equivalent to the single IR sensor employed in a scanning system. By measuring the IR response of all the elements in the flat array simultaneously (or rapidly), the system can record an entire image at once. Image resolution in a staring scanner is limited by the number of elements in the array, whereas in a scanning system it is limited by the size of the scanning dot.

Hybrid designs, in which partial or entire scan-lines are sensed simultaneously by rows of sensors, have also been developed. Chemical films have also proved useful for IR imaging, but these are rarely used today.

The earliest IR imagers, built in the 1940s, 1950s, and 1960s, were scanners. Starers were not technologically feasible until the early 1970s, when large-scale circuit integration made possible the manufacture of focal-plane arrays with good resolution. As integrated-circuit technology has been refined, focal-plane arrays have become cheaper. Starers have many advantages, including greater reliability due to the absence of moving parts, quicker image acquisition, and freedom from internally-produced mechanical vibration.

Formerly, both scanners and starers needed to be cooled by liquid nitrogen in order to keep the sensor from blinding itself with its own IR radiation. In recent years, however, uncooled IR imagers, both scanners and starers, have been increasing in quality and decreasing in price.

**Military applications.** Aircraft, ground vehicles, surface ships, human beings, industrial facilities, rockets, and

warheads entering the atmosphere are some of the objects of military interest that emit IR radiation in telltale patterns. To exploit these patterns, a wide array of military IR systems have been developed. For example, "heat-seeking" missiles that home in on the IR-bright gasses emitted by jet-aircraft engines have been commonplace since the 1950s. Heat-seeking missiles have also been developed for use against surface vehicles and ships. Also, starting in the early 1960s, military IR-imaging satellites have been observing the Earth to detect the IR emissions of rocket and missile launches, and modern proposals for ballistic-missile defense depend heavily on space- and ground-based IR detectors that will track missiles and warheads as they arc through space. The U.S. military is currently designing a new system of satellites dedicated to tracking missiles using IR imaging, the Space Based Infrared System. According to the United States Air Force, this system will have a "unique capability to track missiles throughout their trajectory—not just during the 'hot' boost phase [when IR emissions from the missile are most intense]—allow[ing] the system to effectively cue missile defense systems with accurate targeting data."

Various IR camera systems for "seeing in the dark" are also commonplace. These may be mounted on vehicles or at stationary locations to allow nighttime surveillance of a fixed area. Night-vision systems worn on helmets and mounted on portable weapons usually do *not* operate by sensing IR; instead, they amplify the visible light already present in a dark scene. Hence they are sometimes called "starlight" vision systems.

IR imaging is being investigated for use in the detection of landmines. Antipersonnel mines are typically buried only a few centimeters below the surface, so the heat radiation (IR) pattern of an area can, under some conditions reveal their presence.

**Police and security applications.** The security of a building or area of land from intruders is often enhanced by cameras that image the perimeter of the secure area and can be monitored by personnel in a central office. At night, such systems must either be supplied with illumination or must be capable of IR imaging. Visible-light camera systems are cheaper and easier for human users to interpret; however, because excess illumination of an area by visible light ("light pollution") is sometimes a concern, and because security forces may wish to keep an area under surveillance without making their presence known, IR systems are widely used for perimeter security and other surveillance tasks.

IR imaging has many other uses in police and security work besides surveillance. Aerial IR imaging can track vehicles, show which vehicles in a parking lot have arrived most recently, distinguish heated buildings, and locate buried structures (e.g., clandestine chemical laboratories) emitting heat through vents. IR images can be used to precisely determine the time of death of a person deceased for less than 15 hours or to detect document

forgery by revealing subtle mechanical and chemical disturbances of the original paper and ink. The power consumption in a building can be estimated in real time by observing the IR radiation emitted by the power transformer on the pole outside; modifications to walls or automobiles are often obvious in IR images; and IR images can reveal such visually inconspicuous features of crime scenes as use of cleaning solvents to remove blood, drag-marks across carpets, fresh paint, and explosives residues.

**Countermeasures.** IR imaging, like all surveillance and targeting technologies, has given risen to a thriving countermeasures field. IR countermeasures fall into three broad categories: blinding, decoys, and concealment. Blinding refers to the use of IR lasers to overload an enemy's imaging detectors, as for example those of an approaching missile. Decoys are heat sources released in the vicinity of a target heat source (e.g., aircraft or ship) in order to reduce the chances that an approaching missile will home in on the true target. For example, a system named the AN/ALQ-156(V)2 Missile Approach Detector is standard on several U.S. military aircraft. This system uses radar to scan for approaching heat-seeking missiles. When one is detected, the AN/ALQ-156(V)2 automatically activates the M-130 General Purpose Dispenser System, which releases a flare from the aircraft. The flare emits more IR radiation than the aircraft itself, hopefully distracting the missile from the aircraft.

Since most proposals for ballistic missile defense include interceptor missiles that home in on the heat signature of ballistic warheads approaching from space (and thus IR-bright against a cool background), thought has also been given to the question of "infrared stealth" measures for ballistic-missile warheads. One possibility is "shrouding," which would involve the placement of a close-fitting cap over the cone-shaped warhead. The cap would consist, essentially, of a hollow aluminum shell filled with liquid nitrogen and kept aloof from the warhead itself by insulated supports. The liquid nitrogen would cool the exterior of the warhead, reducing its IR emissions to low levels and making it difficult or impossible for the heat-seeking system of an interceptor missile to locate. The exterior coating of the warhead could be made of a radar-absorbing material, making the warhead radar-stealthy as well.

#### ■ FURTHER READING:

##### BOOKS:

Schlessinger, Monroe. *Infrared Technology Fundamentals*. New York: Marcel Dekker, Inc., 1995.

##### PERIODICALS:

Carter, L. J., et al. "Thermal Imaging for Landmine Detection," in proceedings from Second International Conference on the Detection of Abandoned Land Mines, *IEEE* 110–114, 1998.

Maki, M. C., and M. C. Dickie. "New Options in Using Infrared for Detection, Assessment and Surveillance," in proceedings from the International Carnahan Conference on Security Technology, *IEEE* 12–18, 1996.

Riedel, R. B., J. S. Coffin, and F. J. Prokoski. "Forensic Uses of Infrared Video," in proceedings from the International Carnahan Conference on Security Technology, *IEEE* 108–112, 1992.

#### SEE ALSO

*Night Vision Scopes*

*Strategic Defense Initiative and National Missile Defense*

---

## Infrastructure Protection Center (NIPC), United States National

---

Formerly a unit of the Federal Bureau of Investigation (FBI), the National Infrastructure Protection Center (NIPC) moved to the Department of Homeland Security (DHS) when the latter began its functions in March 2003. NIPC is charged with assessing threats to critical infrastructure—particularly computer systems—and providing warnings concerning threats and vulnerabilities. It also conducts investigations and provides a response to computer attacks.

**NIPC's mission.** Although infrastructure, or critical infrastructure, includes vital systems ranging from roads to banking, the tasks of NIPC are directed toward those computer and information systems that provide much of the control mechanism over other components of the national infrastructure. The mission of NIPC is manifold, though its many components all relate in some way to computers. The NIPC is tasked with detecting, averting, assessing, warning against, responding to, and investigating unlawful acts that target or threaten critical infrastructures in general, and computer and information technologies in particular. It manages investigations of computer intrusion, and supports the response of law enforcement to cyber crimes and computer intrusion.

When incidents of intrusion go beyond the level of crime to that of terrorism or acts of warfare, NIPC works with counterintelligence, counterterrorism, and national security authorities in responding to attacks on interests of the United States. It also coordinates the training of computer investigators and other protectors of infrastructure both in the public and private sectors.

**NIPC at work.** An example of NIPC at work occurred in May 2000, when the "Love Bug" computer worm (a virus-like

program) propagated itself across world computer networks. Within 24 hours, investigators at the New York FBI field office, assisted by NIPC, tracked the virus to Onel de Guzman in the Philippines. Due to the lack of cyber crime statutes in the Philippines, Guzman was not charged, but the incident led to Philippine approval of the international E-Commerce Act, which provides for criminal prosecution of cyber crimes. NIPC has conducted a number of other major investigations against cyber criminals.

The NIPC issues three levels of infrastructure warnings: assessments, which provide general information about non-specific threats; advisories, which address particular dangers that call for preparedness or a change in posture; and alerts, which warn of major and specific threats. In September 2002, for instance, it issued an assessment warning against possible "hactivism" (the use of computer hacking in the service of political activism) connected with upcoming meetings of the International Monetary Fund and World Bank. As of February 2003, NIPC advisory addressed the dangers of global hacking associated with escalating tensions between the United States and Iraq. In August, 2002, NIPC issued an alert based on "credible but nonspecific information" concerning possible cyber attacks originating from Europe. That no problems were reported may be evidence that there was no actual threat—or that NIPC was successful in its job.

#### ■ FURTHER READING:

##### BOOKS:

*Improving Our Ability to Fight Cybercrime: Oversight of the National Infrastructure Protection Center: Hearing Before the Subcommittee on Technology, Terrorism, and Government Information of the Committee on the Judiciary, United States Senate, One Hundred Seventh Congress, First Session, July 25, 2001.* Washington, D.C.: U.S. Government Printing Office, 2002.

*National Infrastructure Protection Center (NIPC): A Public-Private Partnership to Protect America's Critical Infrastructures.* Washington, D.C.: U.S. Department of Justice, 2002.

##### PERIODICALS:

Amon, Michael. "Agencies Working to Boost Security." *Washington Post*. (February 23, 2003): T1.

Johnston, David. "F.B.I. Warns Local Agencies to Be Aware." *New York Times*. (September 10, 2002): A17.

Verton, Dan. "NIPC Warns of Attacks, But No Impact Felt." *Computerworld* 36, no. 33 (August 12, 2002): 17.

———. "NIPC Loses One of Its Own to 'Beltway' Sniper." *Computerworld* 36, no. 43 (October 21, 2002): 6.

##### ELECTRONIC:

National Infrastructure Protection Center. <<http://www.nipc.gov>> (March 4, 2003).

#### SEE ALSO

*Computer Hackers*  
*Computer Hardware Security*  
*Computer Software Security*  
*Critical Infrastructure*  
*Critical Infrastructure Assurance Office (CIAO), United States*

## INS (United States Immigration and Naturalization Service)

■ ADRIENNE WILMOTH LERNER

The United States Immigration and Naturalization Service (INS) was a subsidiary of the Department of Justice. Immigration services are now part of the new Department of Homeland Security. The agency was charged with enforcing laws regulating the immigration of foreign-born individuals, the admission of refugees into the United States, and the naturalization of qualified foreigners wishing to become U.S. citizens. The INS granted tourist, student, and extended stay visas for foreign citizens wishing to visit the United States. Now restructured into the Department of Homeland Security, immigration services are essential in the enforcement of antiterrorism laws and the promotion of national security.

The first federal immigration agency in the United States was established in 1864. At that time, the office was directed to encourage immigration to the United States. Over time, the office evolved as immigration policy changed. By 1890, the government abandoned the "open door policy" and adopted laws restricting the flow of immigrants into the country. The first laws prohibited the entry of people convicted of serious crimes, suffering from contagious diseases, polygamists, and severely mentally ill persons. Later legislation barred immigrants from certain nations and established quotas for immigrants from various regions or countries. As social and political policy changed, so too did the federal immigration agency.

The modern Immigration and Naturalization Service was established in 1933 by Executive Order 6166. The order combined existing separate agencies of immigration and naturalization services. The INS was then part of the Department of Labor. In 1940, the organization was restructured under the President's Reorganization Plan Number V. With the advent of World War II, immigration shifted from being an economic to a security issue. Accordingly, the INS was moved under control of the Department of Justice. The move gave INS more power to adjudicate cases in violation of immigration laws. Furthermore, the INS managed the U.S. border patrol. Border patrol agents

apprehended illegal immigrants and regulated the entry of people into the United States from border crossings and other ports-of-entry.

After the September 11, 2001, attacks on the United States, the INS took a lead role in the strengthening of national security and antiterrorism policy. The agency enacted new guidelines for the issuance of visas, making the general criteria for prolonged entry into the U.S. more stringent. Efforts to satisfy 1996 legislation that mandated the creation of tracking systems to monitor entries and exits from land points of entry have been increased. The controversial Coordinating Interagency Partnership Regulating International Students (CIPRIS), a database that tracks student visa holders, remains largely opposed by the university community, but gained the support of the government as a key means of controlling access to sensitive technology and information.

The INS also gained increased powers of detention and questioning of illegal aliens and visa holders suspected of being connected to terrorist organizations. The period of detention without formal charges was augmented from 24 hours to any reasonable length of time necessary to gather information regarding the case. Mobilization Against Terrorism Act (MATA) granted the INS the power to remove, deport, or prosecute foreign nationals connected to terrorist groups, or who harbor persons connected to such organizations. MATA further applied to foreign nationals granted permanent resident status. Permanent residents also could be detained or deported if certified to be connected with a terrorist group.

Despite these changes to INS operations, the agency was radically restructured under the Homeland Security Act. Former INS duties of border security and immigration services were separated and tasked to separate operational departments under the Department of Homeland Security. The Bureau of Citizenship and Immigration Services (CIS) administers the citizenship program and the granting of visas. Border security is now tasked to the Directorate of Border and Transportation Security (BTS). Screening measures of persons wishing to enter the United States have become more rigorous, as has the enforcement of immigration laws, since the CIS and BTS assumed the powers of the former INS.

U.S. immigration policy is currently based on a preference system that favors skilled workers, professionals, and prospective immigrants from underrepresented nations. Accordingly, one of the main tasks of CIS is to manage the visa selection process efficiently. Refugees fleeing from war or political oppression are handled separately, in conjunction with United Nations and the U.S. Department of Health and Human Services.

The various operational departments of the Department of Homeland Security are also responsible for the apprehension, adjudication, and deportation of criminal aliens. These can be foreign nationals wanted for crimes in their home countries or who have been convicted of a

crime in the United States. In addition, foreign nationals who remain in the United States after their visas expire are considered criminal or illegal aliens, depending on the circumstances of their activities in the U.S. In 2001, immigration services removed nearly 180,000 criminal and illegal aliens, most of whom were apprehended on visa-related violations.

#### ■ FURTHER READING:

##### ELECTRONIC:

Bureau of Citizenship and Immigration Services. INSPASS. March 1, 2003. <<http://www.immigration.gov/graphics/howdoi/inspassloc.htm>> (April 14, 2003).

United States Department of Homeland Security. Bureau of Citizenship and Immigration Services, PORTPASS. March 11, 2003. <<http://www.immigration.gov/graphics/howdoi/portpass.htm>> (April 9, 2003).

United States Department of Homeland Security. Immigration Information, INSPASS. March 4, 2003. <<http://www.immigration.gov/graphics/shared/howdoi/inspass.htm>> (April 9, 2003).

##### SEE ALSO

*United States, Counter-terrorism Policy*

---

## INSCOM (United States Army Intelligence and Security Command)

---

Headquartered at Fort Belvoir, Virginia, the United States Army Intelligence and Security Command (INSCOM) plans and conducts intelligence, security, and information operations for the U.S. Army and its military commanders, as well for the president and other national decisionmakers. Since the time of its establishment in the years immediately after the war in Vietnam, as geopolitical conditions have realigned, INSCOM has been forced to adjust its mission numerous times.

**INSCOM's first quarter-century.** Formed from the old Army Security Agency, INSCOM began its life on January 1, 1977, at Arlington Hall Station in Virginia. This was a time of downsizing for the U.S. military, as America entered a period of relative isolationism, but the crises in Afghanistan and Iran during the late 1970s brought about a resurgence in military growth. In its first seven years, INSCOM grew in strength from 10,400 to 15,000 personnel.

By the mid-1980s, the departure of the Defense Intelligence Agency (DIA) from the Arlington Hall facilities allowed INSCOM to consolidate its headquarters, part of which had been at Fort Meade, Maryland. INSCOM reorganized its five multidiscipline intelligence groups as brigades, and placed a greater emphasis on training its personnel to be warfighters rather than information-gatherers alone. INSCOM relocated to Fort Belvoir in 1989.

**After the Cold War.** That year also saw the beginning of the end of the Cold War, and the decade that followed (1990s) brought considerable change for INSCOM. It was downsized, along with much of the military, and after absorbing the Army Intelligence Agency in 1991, it returned to its earlier emphasis on intelligence-gathering. At mid-decade, it transferred all of its human intelligence operations to DIA.

In the 1990s, INSCOM, like much of the military, found itself tasked with humanitarian operations rather than warfighting. Other unaccustomed activities in the mid-1990s, according to information posted at the INSCOM Web site in 2003, included “supporting treaty verification, conducting counterdrug operations, and protecting the army against an espionage threat posed by nations not traditionally our adversaries.”

**INSCOM today.** September 11, 2001, brought about another phase in the history of INSCOM and the military as a whole. It would be faced with new challenges in a world once again polarized as in the Cold War, but this time with a more enigmatic enemy.

INSCOM had not remained idle during the 1990s; among the new systems it had helped develop were the Sandcrab jammer, the Trackwolf high-frequency direction-finding system, the Trojan Spirit deployable intelligence communications system, the airborne reconnaissance low platform, and the army portion of the Joint Surveillance and Target Acquisition Radar System (J-STARS).

INSCOM consists of four brigades, as well as eight other groups or activities worldwide tasked to specific intelligence disciplines or functions. In all, members of its 14 major subordinate commands and numerous smaller units are in some 180 locations across the globe.

#### ■ FURTHER READING :

##### BOOKS:

Richelson, Jeffrey T. *The U.S. Intelligence Community*, third edition. Boulder, CO: Westview Press, 1995.

##### PERIODICALS:

Girardeau, John H. “Doctrine Corner: INSCOM Intelligence Support to the Tactical Commander.” *Military*

*Intelligence Professional Bulletin* 28, no. 2 (April-June 2002): 56–57.

##### ELECTRONIC:

United States Army Intelligence and Security Command. <<http://www.inscom.army.mil>> (February 2, 2003).

##### SEE ALSO

*Army Security Agency*  
G-2

## INSPASS (Immigration and Naturalization Service Passenger Accelerated Service System)

INSPASS (Immigration and Naturalization Service Passenger Accelerated Service System) is a component of the Port Passenger Accelerated Service System (PORTPASS) in use at selected airports to facilitate passage through entry checkpoints. INSPASS and other expedited U.S. national entry systems are designed to identify preapproved low-risk international travelers using a combination of biometric measurements. Automated entry systems are designed to allow inspectors additional time to focus on high-risk entrants.

As of March 1, 2003, the newly created United States Department of Homeland Security (DHS) absorbed the former Immigration and Naturalization Service (INS). All INS border patrol agents and investigators—along with agents from the U.S. Customs Service and Transportation Security Administration—were placed under the direction of the DHS Directorate of Border and Transportation Security (BTS). Responsibility for U.S. border security and the enforcement of immigration laws was transferred to BTS.

BTS is scheduled to incorporate the United States Customs Service (previously part of the Department of Treasury), the enforcement division of the Immigration and Naturalization Service (previously part of the Department of Justice), the Animal and Plant Health Inspection Service (previously part of the Department of Agriculture), the Federal Law Enforcement Training Center (previously part of the Department of Treasury), Transportation Security Administration (previously part of the Department of Transportation) and the Federal Protective Service (previously part of the General Services Administration).

Former INS immigration service functions are scheduled to be placed under the direction of the DHS Bureau of

Citizenship and Immigration Services. Under the reorganization the INS formally ceases to exist on the date the last of its functions are transferred.

Although the description of the technologies involved in the INSPASS entry security program remains stable, in an effort to facilitate border security BTS plans envision higher levels of coordination between formerly separate agencies and databases. As of April 2003, the specific coordination and future of the INSPASS program was uncertain with regard to name changes, program administration, and policy changes.

INSPASS systems utilize hand geometry biometrics. Hand geometry measurements include biometric registration of hand length, thickness and translucency.

At entry points an INSPASS station compares hand geometry biometric images to a database of preregistered travelers. The INSPASS system is integrated in such a way that data obtained can generate entry records that can be utilized by other monitoring programs. The ability to cross reference databases is a key component in the Department of Homeland Security's emerging strategy to eliminate gaps and spot suspicious activity in entry security systems.

INSPASS also allows travelers to save time. The INSPASS imaging process generally takes less than a minute but still allows positive identification for inspectors. After the prospective entrant's identity is validated, automatic doors or gates open to allow passage. If a file is flagged, more than one person attempts entry, or there is a question of identity, a warning message appears on inspectors' monitors to alert them to a need to conduct a personal interview.

As with other automated entry systems, INSPASS utilizes a "one-to-one" search protocol to verify identity. Instead of comparing gathered biometrics across a broad database, an identification number allows direct comparison with the biometric measurements on file for that identification number. In essence, the automated systems only verify that the person is the same person initially associated with the biometric measurements on file in the database. Unlike fingerprint search protocols used by the FBI, the entry search protocols are, as of March 2003, unable to take biometrics and conduct a broad search to identify a subject's identity. In theory, the same biometric measurements could be registered to two different identities.

As of March 2003, the airport INSPASS was available at airports in New York, Newark, San Francisco, Los Angeles, Miami, and some Canadian sites.

INSPASS is available to citizens and lawful permanent residents of the United States, citizens of Canada or Bermuda, and landed immigrants of Canada who are citizens of British Commonwealth countries. Citizens of Visa Waiver Pilot Program countries are also eligible. Applicants for the airport INSPASS must travel to the

United States on business at least three times per year. In addition to other restrictions, INSPASS is not available to travelers who have a criminal record.

The legal basis of all entry inspections derives from the Immigration and Nationality Act (INA) and the Code of Federal Regulations [CFR].

Other countries have similar automated immigration systems. For example, Canada uses the CANPASS system (Canadian Passenger Accelerated Service System).

■ FURTHER READING:

ELECTRONIC:

- Bureau of Citizenship and Immigration Services. INSPASS. March 1, 2003. <<http://www.immigration.gov/graphics/howdoi/inspassloc.htm>> (April 14, 2003).
- Department of Homeland Security. April 2, 2003. <<http://www.dhs.gov/dhspublic/index.jsp>> (April 11, 2003).
- United States Department of Homeland Security. Bureau of Citizenship and Immigration Services, PORTPASS. March 11, 2003. <<http://www.immigration.gov/graphics/howdoi/portpass.htm>> (April 9, 2003).
- . Immigration Information, INSPASS. March 4, 2003. <<http://www.immigration.gov/graphics/shared/howdoi/inspass.htm>> (April 9, 2003).

SEE ALSO

- APIS (Advance Passenger Information System)*
- IBIS (Interagency Border Inspection System)*
- IDENT (Automated Biometric Identification System)*
- NAILS (National Automated Immigration Lookout System)*
- PORTPASS (Port Passenger Accelerated Service System)*
- SENTRI (Secure Electronic Network for Travelers' Rapid Inspection)*

---

## Inspector General (OIG), Office of the

---

The Office of the Inspector General (OIG) is part of the United States Department of State and serves as a reviewer of department operations. The office also handles claims of government fraud, waste, and abuse, whether reported by department personnel or outside sources. The inspector general is responsible for briefing the executive branch and Congress on oversight issues, as well as coordinating investigations undertaken by the inspection offices of other Federal departments.

One of the main subsidiaries of the OIG is the Office of Security and Intelligence Oversight. The oversight committee routinely examines the administration of intelligence and security programs. The inspections serve the

overall Department of State responsibility of providing international security for U.S. personnel, information, economic interests, and property. More recently, special attention has been paid to the assessment of terrorism threats and counter-terrorism readiness plans in U.S. offices abroad.

The OIG also investigates general forms of government malpractice, such as embezzlement, theft of government property, abuse of power or position, and misconduct. If sufficient case evidence is found during an OIG investigation, the case can be recommended to legislative oversight committees or the Federal Bureau of Investigation (FBI) if necessary.

Other government departments have their own internal offices of Inspector General. Like that of the Department of State, some of these serve important functions in the greater intelligence community. The Inspector General of the Department of Energy aids the National Nuclear Security Administration, the commission responsible for assessing the current age, state, and safety of the U.S. nuclear arsenal. In 2002, the Inspector General of the Treasury aided congressional investigations of large-scale corporate fraud and carried out a major review of the security structure protecting credit information and electronic funds transfers.

Many duties of the Office of the Inspector General coincide with those of the Department of Homeland Security. As the new department is established and grows, the umbrella structure surrounding the OIG will likely change.

#### SEE ALSO

*Homeland Security, United States Department of*

## Intelligence

Intelligence is information concerning a foreign entity, usually (although not always) an adversary, as well as agencies concerned with collection of such information. It is intimately tied with the intelligence cycle, a process whereby raw information is acquired, converted into intelligence, and disseminated to the appropriate consumers.

The intelligence cycle, as defined in the United States Senate hearings of the Church Committee during the mid-1970s, consists of four or five steps. In the first of these, called either *planning*, *direction*, or *planning and direction*, intelligence requirements are determined, a plan for the collection is developed, and agencies are assigned to specific collection tasks. Throughout the intelligence cycle, this first step recurs in the form of continued checking on the productivity of collecting agencies.

The second step, *collection*, is probably the one that most readily comes to mind when the average person thinks of intelligence. Collection involves actions the layperson would call “spying.” Collection includes the gathering of information through means such as surveillance of various types, as well as the cultivation of human contacts. Through these and other means, information sources are exploited, and this information is delivered to the appropriate processing unit.

The third and fourth steps, *processing* and *production*, are sometimes viewed as a single step. In the processing phase, raw data is converted into a more usable form; then that information is evaluated, analyzed, integrated, and interpreted to produce what is no longer mere information, but true intelligence. Suppose numerical data on a factory’s output is collected; in the processing phase, these numbers may be put into the form of a graph, while in the production phase, an analyst determines overall patterns and what they mean.

Finally, there is *dissemination*, the step in which processed intelligence is distributed to the appropriate consumers, which are usually government or military officials.

#### ■ FURTHER READING:

##### BOOKS:

Martin, David C. *Wilderness of Mirrors*. New York: Harper & Row, 1980.

Polmar, Norman, and Thomas B. Allen. *Spy Book: The Encyclopedia of Espionage*. New York: Random House, 1998.

Richelson, Jeffrey T. *The U.S. Intelligence Community*, fourth edition. Boulder, CO: Westview Press, 1999.

Wright, Peter. *Spycatcher: The Candid Autobiography of a Senior Intelligence Officer*. New York: Viking, 1987.

##### SEE ALSO

*Espionage*

*HUMINT (Human Intelligence)*

*Intelligence Agent*

*Intelligence and Counter-Espionage Careers*

*Intelligence Community*

*Intelligence Officer*

*Measurement and Signatures Intelligence (MASINT)*

*SIGINT (Signals Intelligence)*

## Intelligence Agent

#### ■ JUDSON KNIGHT

In general terms, an agent is one authorized to act in place of, or on behalf of, another. An intelligence agent, however, is not simply an agent of or for an intelligence

agency. Whereas members of the agency are called intelligence officers, operatives, or special agents, an agent is someone hired or recruited from outside. There are numerous other variations in the informal taxonomy of agents, including secret or undercover agents, agents provocateur, agents-in-place, double agents, and agents of influence.

**The distinction between agents and operatives.** Intelligence agency employees who work in the field do not call themselves agents; an agent is someone hired or recruited by an intelligence agency to do its bidding. The person to whom the agent reports—the actual agency employee—is known as an operative.

The distinction goes back to World War II and the origins of modern intelligence agencies. At that time, Office of Strategic Services (OSS) manuals defined an operative as “an individual employed by and responsible to the OSS and assigned under special programs to field activity.” An agent, on the other hand, was defined by OSS as “an individual recruited in the field who is employed or directed by an OSS operative.” The Central Intelligence Agency (CIA), successor to OSS, calls its operatives CIA officers.

There are numerous variations on the term “agent.” In the Federal Bureau of Investigation (FBI) under J. Edgar Hoover, operatives called themselves “special agents.” By this designation, Hoover meant to distinguish FBI agents from ordinary police officers.

**Secret agents, double agents, and agents-in-place.** A *secret agent* or *undercover agent* is, simply enough, an agent who works in a clandestine capacity, such that the relationship with the intelligence agency is not obvious to those around him or her. These terms are more likely to show up in the vocabulary of laypeople than of intelligence operatives. In fact, such terminology is somewhat redundant, inasmuch as most agents must be secret or undercover in order to function effectively.

More useful are terms such as *double agent* or *agent-in-place*. A double agent is someone who seems to serve one intelligence agency, but actually works on behalf of another. Usually these agencies represent enemy governments, and the double agent provides information to one agency about the other or others. If, instead of two agencies, an agent serves three, the term *triple agent* is used. The double or triple agent may even be providing information to each service about the others, but usually there is only one entity that the double agent truly or ultimately serves.

A double agent whose perfidy has been discovered by the agency against which he or she is spying, and who is then used in that agency’s service against the other, is a *redoubled agent*. An agent may be forced against his or her will to become a double agent. The same is true of a

redoubled agent, a role an agent can assume without even knowing that he or she is doing so—for example, by being given inaccurate or deliberately deceptive material to pass on as genuine intelligence.

An agent-in-place is similar to a double agent, with the difference that, whereas a double agent is usually called upon by agency to take that role, the agent-in-place usually volunteers for the position. Suppose a person works for Agency A, then is sent to work for agency B so as to report information to Agency A without anyone at Agency B knowing. That is a double agent. On the other hand, an agent-in-place would be someone working for Agency B who, of his or her own initiative, offered services to Agency A. The agent would continue to work for Agency B, and feed information to Agency A.

An agent-in-place is extremely valuable to the employing agency, but his or her role has great risks. For agents in place working on behalf of America’s enemies—for example, Robert Hanssen, the FBI special agent who sold secrets to the Soviets and later the Russians—discovery led to imprisonment. For agents-in-place working on behalf of America in the Soviet camp, the penalty for discovery was far worse. According to an anecdote reported by Henry Becket, when KGB officers discovered that one of their own was serving the Americans as an agent-in-place, he was thrown feet first into a roaring furnace while his colleagues watched.

**Sleepers, provocateurs, and agents of influence.** Several other interesting variations on the concept of an agent are sleeper agents, agents provocateur, and agents of influence. A *sleeper agent* is one placed in an undercover situation and told to await further instructions before beginning to actively engage in espionage activities. A sleeper may remain inactive for months or years, or even the rest of his or her life.

An *agent provocateur* is someone who infiltrates a group or organization with the purpose of inciting its members to unlawful acts that would bring them to the attention of—and most likely cause them to receive punishment from—authorities. Agents provocateur in labor organizations of the late nineteenth or early twentieth centuries, for instance, instigated mob violence that brought police action against workers’ groups.

Finally, an *agent of influence* is someone who does not directly work for an intelligence agency, but is willing to act on its behalf. For example, right-leaning American intellectuals during the mid-twentieth century who worked for the Congress of Cultural Freedom, a CIA-sponsored group intended to influence western European opinion during the Cold War, often knowingly acted as agents of influence for U.S. intelligence. At the same time, many left-leaning Western intellectuals who were fed Soviet propaganda or disinformation, and who disseminated that material as truth, unwittingly acted as agents of influence for the KGB.



## ■ FURTHER READING :

### BOOKS:

Bennett, Richard M. *Espionage: An Encyclopedia of Spies and Secrets*. London: Virgin Books, 2002.

Nash, Jay Robert. *Spies: A Narrative Encyclopedia of Dirty Deeds and Double Dealing from Biblical Times to Today*. New York: M. Evans, 1997.

Richelson, Jeffrey T. *The U.S. Intelligence Community*, fourth edition. Boulder, CO: Westview Press, 1999.

### SEE ALSO

*CIA, Formation and History*

*Hanssen (Robert) Espionage Case*

*Intelligence*

*Intelligence Officer*

*KGB (Komitet Gosudarstvennoi Bezopasnosti, USSR Committee of State Security)*

*OSS (United States Office of Strategic Services)*

---

## Intelligence and Counterespionage Careers

---

### ■ JUDSON KNIGHT

There is no single template for a career in intelligence and espionage. Three of the nation's leading intelligence organizations—the Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), and National Security Agency (NSA)—hold a wide array of opportunities in areas ranging from science, engineering, and mathematics, to linguistics, cartography, and foreign analysis. For each agency, career choices are naturally geared for the tasks at hand, with the NSA, for instance, concentrating on mathematics and cryptography, and the FBI focused on law enforcement. Nevertheless, opportunities are varied, though requirements, which call for extensive background checks, are high.

### The CIA

Intelligence agencies have always been, by their nature, secretive. During the Cold War, this secrecy extended to their personnel requirements and practices. Today, however, while computerized encryption and other forms of technology maintain a higher level of secrecy than ever, where vital intelligence information is concerned, the CIA and other agencies are remarkably open about matters such as hiring.

The CIA, which regularly publishes declassified studies of past operations (some of them highly critical of CIA

activities), has been a leader in establishing a tradition of openness among intelligence agencies. In 1998, it even took out newspaper advertisements to recruit talented personnel for what the ads called “the ultimate international career for the extraordinary individual.” Since that time, Israel's Mossad has also undertaken a recruiting effort.

Despite the scaling back of CIA resources following the end of the Cold War, director of recruitment Gil Medeiros told the media in 1998, “We found no lessening of tasking to the agency. We had to face the fact that it takes people in the field to do human sourcing intelligence.” Soon the CIA also had in place job listings at its Web site, where it listed dozens of possible professions within the organization. Many of these fit under one of several categories: analytical positions; language positions; scientists, engineers, and technologists; and “clandestine service.”

**CIA jobs and the intelligence cycle.** Most jobs in intelligence relate to some particular point in the intelligence cycle, a process whereby raw information is acquired, converted into intelligence, analyzed, and disseminated to the appropriate consumers. The acquisition in the field may be most familiar to civilians, but a much greater amount of activity is involved in the conversion of raw data into intelligence.

Among the areas of specialty the CIA uses in the processing and production phases of the intelligence cycle are various language and analytical skills. Within language skill areas, demands in 2003 were highest for Arabic and Korean, a reflection of the efforts against terrorism in the Middle East and weapons proliferation in North Korea at that time. The CIA also called for instructors and foreign media analysts with abilities in a variety of languages. Among the analytical positions advertised in 2003 were statisticians, as well as analysts specializing in China, the Middle East, the military, counterintelligence threats, and counterterrorism.

In acquiring, processing, and disseminating information, the CIA calls on the skills of scientists, engineers, and technologists. Advertised positions in 2003 ranged from mechanical, civil, electrical, and materials engineers to software specialists, signals intelligence officers, and even textile specialists.

The CIA also advertised opportunities in what it referred to as “clandestine service,” including the positions of operations officer and language officer. Additionally, it has an ongoing need for a range of other professional personnel, including architects, attorneys, cost estimators, geographers, graphic designers, human resource consultants, medical officers, nurses, paralegals, physicians, psychiatrists, psychologists, video production specialists, and many others.

The agency offers a number of opportunities for college students, including a generous scholarship program (up to \$15,000 yearly in 2003) for qualifying applicants



Students at the FBI Academy in Quantico, Virginia, learn techniques for subduing suspects. ©ANNA CLOPET/CORBIS.

majoring in electrical engineering or computer science. Requirements include U.S. citizenship, an SAT (Scholastic Aptitude Test) score of 1000 or above, a grade point average of 3.0 or better, and demonstrated financial need. Internships are also available, as are student trainee and graduate studies programs, all of which require at least temporary relocation to the Washington, D.C., area.

## NSA

Although it is a much more secretive organization than the CIA in many regards, the NSA has a number of available positions, and is known as both the largest employer in Maryland and the largest employer of mathematicians in the United States. Its areas of specialty as of 2003 included language and intelligence analysts, electronic and computer engineers, and systems analysts and computer scientists, mathematicians, and cryptanalysts.

Prospective employees in any sensitive government position must expect a fairly extensive process of background checks, and nowhere is this more apparent than with NSA. Employment of any kind with NSA requires that an individual obtain a high-level security clearance. Applicants should expect to undergo medical screening, a polygraph interview, and a background investigation that

will open up past financial dealings and other details that a private citizen would consider personal business.

NSA employees do not enjoy the same privacy rights as ordinary citizens: overseas travel, plans to marry a non-U.S. citizen, even one's choice of a doctor or dentist, must be submitted for approval. (In the case of the doctor or dentist, this is because the employee might reveal secrets while under anaesthesia.) In addition, NSA employees, like many others in government positions, must submit to random drug testing. On the other hand, NSA is willing to consider persons with dual citizenship, though dual citizenship raises potential issues that must be addressed on an individual basis. All NSA new-hires must relocate to NSA headquarters at Fort Meade, Maryland.

## The FBI

Within the FBI, the most visible position is that of special agent, but the bureau also offers an array of professional, administrative, technical, and clerical positions. Among the specific positions for which the bureau has a continuing need are attorneys, intelligence research specialists, and secretaries. Other examples of professional support personnel with the FBI include financial analysts, program analysts, computer specialists, nurses, auditors, language specialists, and photographers.

All applicants for professional support personnel positions must be U.S. citizens, with at least a high school diploma, as well as college or graduate degrees appropriate to particular areas of specialty. They must undergo a background investigation with a duration of between one and four months, during which time investigators will contact former and current employers, personal references, friends, neighbors, and family members. FBI personnel will also review school, credit, arrest, medical, and military records of prospective employees.

Special-agent applicants must be U.S. citizens, at least 23 years of age, but younger than 37. They must possess a four-year degree from an accredited college or university, as well as a valid driver's license, and must pass polygraph, drug, and color vision tests. Uncorrected vision must not be worse than 20/200 in one eye, and 20/40 in the other. If accepted for employment, they will undergo 16 weeks of intensive training at the FBI Academy in Quantico, Virginia, where they will receive 708 instructional hours in areas that include academics, firearms, physical training, defensive tactics, and practical exercises. Following graduation, special agents will undergo a two-year probationary period.

Once hired, an employee can expect to spend four years in the first office of assignment. For a special agent who has spent 10 years at the same office, a non-voluntary rotational transfer to a second field office will most likely take place. Some professional support positions, such as that of language specialist or investigative specialist, may call for temporary duty or short-term transfers.

#### ■ FURTHER READING:

##### BOOKS:

Phillips, David Atlee. *Careers in Secret Operations: How to Be a Federal Intelligence Officer*. Frederick, MD: University Publications of America, 1984.

##### PERIODICALS:

Boyle, Matthew. "The Prying Game." *Fortune*. (September 17, 2001): 235.

Lang, John. "CIA Ads Tout Career in Espionage." *Dallas Morning News*. (November 1, 1998): 15A.

##### ELECTRONIC:

Careers in Intelligence. Association of Former Intelligence Officers. <<http://www.afio.com/sections/careers/>> (April 30, 2003).

CIA Careers. Central Intelligence Agency. <<http://www.cia.gov/employment/>> (April 30, 2003).

Employment. Federal Bureau of Investigation. <<http://www.fbi.gov/employment/employ.htm>> (April 30, 2003).

NSA Career Center. National Security Agency. <<http://www.nsa.gov/programs/employ/homepage.html>> (April 30, 2003).

Online Career Center. Intelligence Careers. <[http://www.intelligencecareers.com/\\_homeroom/index.cfm](http://www.intelligencecareers.com/_homeroom/index.cfm)> (April 30, 2003).

#### SEE ALSO

*CIA (United States Central Intelligence Agency)*  
*Classified Information*  
*Crime Prevention, Intelligence Agencies*  
*FBI (United States Federal Bureau of Investigation)*  
*Intelligence Community*  
*Law Enforcement Training Center (FLETC), United States Federal*  
*Mossad*  
*NSA (United States National Security Agency)*  
*Privacy: Legal and Ethical Issues*  
*Security Clearance Investigations*  
*United States, Intelligence and Security*

## Intelligence and Democracy: Issues and Conflicts

■ TIMOTHY G. BORDEN

There have always been conflicts between individual rights and national security interests in democracies. Limits on civil liberties during wartime, including restrictions on free speech, public assembly, and mass detentions, have been the most serious threats to individual freedom. Even in peacetime, counter-terrorist measures including profiling, detention, and exclusion, along with the use of national identification cards, have raised concerns about racism, constitutional violations, and the loss of privacy. With the passage of new anti-terrorist laws after September 11, 2001, these tensions have increased. Supporters of broader governmental powers insist that they are part of the increased security measures necessary to safeguard national security. In contrast, many civil rights groups fear that the infringement upon individual rights is another step in the erosion of democratic civil society.

**Wartime measures.** The severest restrictions on civil liberties have occurred in times of war. In September 1862, during the American Civil War, President Abraham Lincoln (1809–1865) suspended the right of *habeas corpus* in order to allow federal authorities to arrest and detain suspected Confederate sympathizers without arrest warrants or speedy trials. Well aware of the drastic nature of such a step, Lincoln justified it as a necessary wartime measure. After the United States Supreme Court found Lincoln's abrogation of *habeas corpus* an unconstitutional intrusion on Congressional authority, Congress itself ratified the measure by passing the *Habeas Corpus Act* in September 1863. Through 1864, about 14,000 people were arrested under the act; about one in seven were detained at length in federal prisons, most on allegations of offering aid to the Confederacy but others on corruption and fraud charges.

Generations of historians have debated whether the suspension of a basic constitutional right such as *habeas corpus* was indeed justified, even though Article 1, Section 9, of the Constitution allowed *habeas corpus* to be suspended "in cases of rebellion or invasion" in the name of public safety. The controversy continued through the Reconstruction Era (1866–1876) and the passage of the Ku Klux Klan Act of 1871, which reiterated the use of federal military intervention and suspension of *habeas corpus* to force state officials to secure voting rights, jury service, and equal protection under the law for all citizens regardless of race. When Reconstruction ended in 1876, the law quickly fell into disuse.

Another major conflict between individual rights and national security and intelligence interests occurred during World War I. Although President Woodrow Wilson (1856–1924) had campaigned in 1916 on a platform of keeping the United States out of the conflict that raged in Europe, public sentiment against the Central Powers, led by Germany and Austria-Hungary, grew after sensational reports surfaced of German atrocities against civilians and a plot to inveigle Mexico to join the war against the United States. Wilson responded by instituting a peacetime military draft in July 1917, and persuading Congress to pass the Espionage Act that same year. Amended by the Sedition Act of 1918, the Espionage and Sedition Acts broadened the arrest powers granted to federal agents in apprehending and detaining individuals suspected of treason or antiwar activity. About 1,500 people were arrested under the acts for refusing to comply with the draft, publicly criticizing American foreign policy, and voicing opposition to America's involvement in the war. The Industrial Workers of the World union and Socialist Party came under particular scrutiny, given their antiwar platforms; the Socialist Party even had its newspapers banned from the U.S. mail because of their antiwar editorials and reports. Socialist Party leader Eugene V. Debs (1855–1926) was also convicted and sentenced to a ten-year prison term under the Espionage Act for an antiwar speech he gave in Canton, Ohio, in June 1918. Debs was later pardoned by President Warren G. Harding (1872–1936) in December 1921.

After the conclusion of World War I in November 1918, the federal government continued to use the Espionage and Sedition Acts as the basis for mass arrests and intelligence gathering. The Russian Revolution of 1917 and the brief takeover of the Hungarian government in 1919 by communists, as well as the presence of an estimated 40,000 Communist Party members in the United States, fueled concerns by authorities over the potential threat of communist-inspired unrest. The fears increased after anarchist groups targeted several government and business leaders with bombs in April and May of 1919, a terrorist wave that culminated in a series of bombings in eight American cities on June 2, 1919. Under the orders of Attorney General A. Mitchell Palmer, federal agents began rounding up suspected communists and anarchists in November 1919. The Palmer Raids, as they became known,

lasted until March 1920, and resulted in the arrest of 6,000 suspects. Palmer then announced that he had uncovered an anarchist-organized plot to stage a wave of violence on May Day, 1920. The day passed without incident and America's first "Red Scare" faded away, only to reappear later under McCarthyism.

The largest detainment of American citizens in the name of national security occurred with the internment of 110,000 Japanese-Americans during World War II. In the two months after the Japanese attack on Pearl Harbor on December 7, 1941, the U.S. Department of Justice ordered the detention of about 2,200 Japanese; 1,400 German; and 269 Italian nationals. After considering a large-scale roundup of all alien residents from the Axis Powers, the government decided to place Italian nationals under travel restrictions and prohibited them from using short-wave radios and owning guns. The restrictions on resident aliens from Italy were abandoned by the end of 1942. Fewer limits were placed on German resident aliens, although 254 of them were banned from specific military areas for security reasons.

In contrast, the 47,000 Issei living in the United States, Japanese-born residents who were barred under federal law from gaining American citizenship, and 80,000 of their American-born family members, called Nissei, were subjected to internment under Executive Order 9066, signed by President Franklin D. Roosevelt (1882–1945) in February 1942. The Roosevelt administration cited national security and sabotage risks for the decision, but exempted almost all of the ethnic Japanese living in Hawaii, whose freedom was vital to the island's economic survival. The mass detention was upheld by a U.S. Supreme Court ruling and was not lifted until December 1944. In 1988, Congressman Norman Y. Mineta, a former detainee, sponsored the Civil Liberties Act, which granted a payment of \$20,000 to each detainee. Most contemporary scholars agree that the Japanese internment camps were not justified by intelligence or security demands, but were motivated by wartime hysteria, racism, and political lobbying by California farmers, who resented the success that some Japanese immigrants had as growers and gardeners in the region.

**Peacetime measures: The FBI and CIA.** Although the United States and Soviet Union were nominally allies during World War II, a resumption of anticommunist sentiment characterized the American political scene after the war. The Taft-Hartley Act of 1947 banned members of the Communist Party from holding leadership positions in American labor unions, and the continuing investigations by the U.S. House Un-American Activities Committee (HUAC) regularly made headlines. The 1950 McCarran Act required all Communist Party members to register with the U.S. Attorney General and allowed the U.S. Justice Department to arrest and detain resident aliens who were subject to deportation hearings. The Federal Bureau of Investigation (FBI) participated in the growing Red Scare by conducting another roundup of suspected Communist

agents, using the powers it retained under the 1940 Smith Act, which permitted the arrest of any individual inciting the overthrow of the government.

The leading anticommunist crusader was Wisconsin Senator Joseph McCarthy (1908–1957), who accused the U.S. State Department of being infiltrated with communist spies in a speech before a West Virginia audience in February 1950. McCarthy's charges stunned the nation, even though it was later proved that he had fabricated them. Under McCarthyism, as the period came to be known, hundreds of government workers were fired as a result of so-called loyalty investigations. In the Senate's Army-McCarthy Hearings in 1954, it was revealed that McCarthy had launched an investigation of the Army after it had rejected one of his aides for a commissioned post, and the Senator's public support diminished. Later censured by the Senate, McCarthy died in 1957 as a symbol of the worst excesses of America's anticommunist hysteria.

Despite the controversies engendered by the role of the FBI and Central Intelligence Agency (CIA) during the McCarthy era, it was not until the 1960s that the agencies came under intense scrutiny for their practices. The FBI was widely praised for its investigation of crimes against civil-rights activists during the decade, yet its infiltration of students' and antiwar groups, particularly those opposed to America's involvement in the Vietnam War, raised suspicions that it routinely violated the constitutional rights of American citizens. The CIA, officially established in 1947, also came under criticism for its involvement in overthrowing foreign governments that were perceived as being hostile to the United States, especially if they were aligned with the Soviet Union. The failed Bay of Pigs invasion of Cuba in 1961 with a group of CIA-trained Cuban exiles was a major embarrassment to the Kennedy administration and was later cited as an example of the disregard of American intelligence agencies for international law. Reforms in the 1970s put stricter limits on the activities of both the FBI and CIA, including narrower prerogatives for collecting intelligence, conducting operations, and initiating covert activities.

### Intelligence and democracy conflicts around the world.

Democratic countries other than the United States have also faced the conflict between maintaining the individual rights of their citizens and conducting vital intelligence and security operations. While the United States government moved to reassure the public that its civil liberties would be safeguarded, however, some nations have responded somewhat differently in the face of imminent terrorist threats.

The threat of terrorist attacks by its neighbors had been a constant presence in Israeli life, particularly since the first bombings by the Palestine Liberation Organization (PLO) in 1965. The PLO's terrorist campaign against Israel became acute during its Intifada (or "shaking off") of Israeli authority in the Occupied Territories in 1987 and again in 2001. Ranking the threat of terrorism as one of the

state's most pressing concerns, Israeli law allowed the indefinite detention of suspected terrorists without trial and forbid public shows of support for terrorist groups. Although the measures were condemned by some in the international community as selectively applied against non-Israelis, the country's leaders consistently defended the practices as a necessity for survival in the face of imminent and ongoing terrorist threats.

The United Kingdom has also faced international criticism for its actions against the Irish Republican Army's violence in protest of the British presence in Northern Ireland. Under the Prevention of Terrorism Act of 1974, British authorities could arrest suspected terrorists without a warrant and detain them for a week without bringing charges against them. While being interned, detainees were subjected to a range of harsh practices that included "hooding"—being isolated and forced to wear a hood over their heads—noise bombardment, and sleep and food deprivation.

**Post-September 11 developments.** After the terrorist attacks of September 11, 2001, on the United States, the government moved to enact stricter counter-terrorist measures that once again raised concerns about the sanctity of individual civil liberties. On October 26, 2001, President George W. Bush signed the Patriot Act into law, giving the FBI and CIA broader investigatory powers and allowing them to share confidential information about suspected terrorists with one another. Under the act, both agencies could conduct residential searches without a warrant and without the presence of the suspect and could seize personal records on the spot. The provisions were not limited to investigating suspected terrorists, but were allowed in any criminal investigation. The Patriot Act also granted the FBI and CIA greater latitude in using computer tracking devices such as the Carnivore (DCS1000) to gain access to Internet and phone records.

The United Kingdom also passed a new counter-terrorist bill in December 2001, the Anti-Terrorism, Crime, and Security Act. The act allowed authorities to detain suspected terrorists for up to six months before reviewing their cases and for additional six-month periods after that. As in the United States, watchdogs in the United Kingdom criticized the new law for potentially infringing upon a basic civil liberty, in this case the right to avoid unlawful detention and gain access to a speedy trial.

The controversy over post-September 11, 2001, measures also extended to the screening of passengers on commercial airlines. The Computer Assisted Passenger Prescreening System (CAPPS), which had been selectively used before September 11, now came into wider usage in American airports. CAPPS looked at numerous factors to determine whether a passenger represented an elevated risk of being a terrorist, including how the plane ticket was bought, whether it was a round-trip or one-way ticket, and where the flight originated, and a 2001 U.S.

Department of Justice review ruled that it was not discriminatory. Despite this reassurance, some Arab rights groups maintained that CAPPs unfairly singled out individuals of Arab descent based on racial profiling.

## ■ FURTHER READING:

### BOOKS:

- Conroy, John. *Unspeakable Acts: The Dynamics of Torture*. New York: Alfred A. Knopf, 2000.
- Hewitt, Christopher. *Understanding Terrorism in America*. New York: Routledge, 2002.
- Heymann, Philip B. *Terrorism and America: A Common-sense Strategy for a Democratic Society*. Cambridge, MA: MIT Press, 1998.
- Michel, Lou, and Dan Herbeck. *American Terrorist: Timothy McVeigh and the Oklahoma City Bombing*. New York: Regan Books, 2001.
- Rehnquist, William H. *All the Laws But One: Civil Liberties in Wartime*. New York: Alfred A. Knopf, 1998.
- Schrecker, Ellen. *Many Are the Crimes: McCarthyism in America*. Boston: Little, Brown and Company, 1998.

### SEE ALSO

*Airline Security*  
*Assassination*  
*Biological and Toxin Weapons Convention*  
*Biological Warfare*  
*Bioterrorism*  
*Bioterrorism, Protective Measures*  
*Bugs (microphones) and Bug Detectors*  
*Church Committee*  
*CIA (United States Central Intelligence Agency)*  
*CIA, Legal Restriction*  
*Classified Information*  
*Cold War (1945–1950): The Start of the Atomic Age*  
*Cold War (1950–1972)*  
*Cold War (1972–1989): The Collapse of the Soviet Union*  
*Commission on Civil Rights, United States*  
*Continuity of Government, United States*  
*Covert Operations*  
*Dirty Tricks*  
*Espionage Act of 1917*  
*FBI (United States Federal Bureau of Investigation)*  
*FOIA (Freedom of Information Act)*  
*Foreign Intelligence Surveillance Court of Review*  
*Intelligence, United States Congressional Oversight*  
*Internet Spider*  
*Internet Tracking and Tracing*  
*Interrogation*  
*Interrogation: Torture Techniques and Technologies*  
*Iran-Contra Affair*  
*Israel, Counter-terrorism Policy*  
*Israel, Intelligence and Security*  
*Justice Department, United States*  
*McCarthyism*  
*Official Secrets Act, United Kingdom*  
*Patriot Act Terrorist Exclusion List*  
*Patriot Act, United States*  
*Politics: The Briefings of United States Presidential Candidates*  
*President of the United States (Executive Command and Control of Intelligence Agencies)*  
*Privacy: Legal and Ethical Issues*

### Profiling

*Telephone Recording Laws*  
*United Kingdom, Counter-terrorism Policy*  
*United States, Counter-terrorism Policy*  
*United States, Intelligence and Security*  
*Watergate*

## Intelligence and International Law

■ JUDSON KNIGHT

The principal statutes of international law guiding intelligence operations are the laws of war established by the conferences at The Hague in The Netherlands in 1899 and 1907, and by a series of conventions in Geneva, Switzerland, between 1864 and 1975. Particularly significant are the 1907 Hague Land Warfare Regulations and the third and fourth Geneva Conventions of 1949, which address treatment of prisoners of war (POWs), spies, and mercenaries. U.S. actions to combat terrorism and terror-supporting entities following the September 11, 2001, attacks prompted a national and international debate over the application of international law.

## The Framework of International Law

The term “international law” is somewhat misleading, inasmuch as *law* usually implies a system to which its subjects are required to submit, whether they agree to it or not. International law, on the other hand, rests almost entirely on the consent of nations to abide by that law, and the willingness of signatories to enforce it through sanctions, military actions, or other means. International law governs rules of peace, war, and neutrality. Laws of peace address matters such as the recognition of one nation by another, as well as guarantees of territorial sovereignty and the extent of territorial waters. Laws of neutrality prevent combatants in a war from moving troops or material across neutral territory, while laws of war govern treatment of combatants, civilians, medical personnel, and POWs in wartime.

**Geneva 1864 and the Hague conferences.** The concept of international law dates back to the writings of seventeenth-century Dutch statesman Hugo Grotius, who established the principle that nations should abide by conventions of conduct. The first significant attempt to establish a body of international law occurred when 12 nations met in Geneva in 1864. The first Geneva Convention, which addressed “the amelioration of the condition of the

wounded on the field of battle," resulted in principles for protecting noncombatant personnel caring for the wounded, and established the International Red Cross.

During two conferences held at The Hague in 1899 and 1907, a much larger body of nations—44 in the case of the 1907 Hague Peace Conference—signed a total of 14 conventions governing laws of war, peace, and neutrality. The 1899 Hague Convention established a Permanent Court of Arbitration, which became the Permanent Court of International Justice under the League of Nations following World War I. The United Nations, established after World War II, changed its name to the International Criminal Court, but it is known popularly as the World Court.

**Laws on treatment of POWs.** During the period from 1928 and 1975, a series of Geneva Conventions addressed a number of issues relating to warfare, including the use of chemical and bacteriological weapons, as well as the treatment of POWs. These, along with the earlier Hague agreements, established the principles whereby intelligence could and could not be gathered from combatants. Particularly significant in this regard were the third and fourth Geneva Conventions of 1949, often referred to as Geneva Conventions III and IV.

According to Article 17 of Geneva Convention III, POWs are required to provide interrogators only with surname, first name, rank, date of birth, identification number, or equivalent information. The same article states that "No physical or mental torture, nor any other form of coercion, may be inflicted on prisoners of war to secure from them information of any kind whatever." Article 31 of Geneva Convention IV prohibits the use of torture against civilians "in particular to obtain information from them or from third parties."

On the other hand, Article 24 of the 1907 Hague Land Warfare Regulations notes that "measures necessary for obtaining information about the enemy and the country are considered permissible"—a recognition of the fact that nations will conduct intelligence operations in wartime. Protocol I, Article 46 states that military personnel gathering intelligence while in uniform are to be accorded the treatment due other combatants, but expressly withholds these protections from undercover operatives or agents captured while in the act of conducting espionage. Article 47 similarly exempts mercenaries—those who fail to meet standards of lawful combatants established by Article 44 of 1907 Conference—from the rights of POWs. A similar provision exists in Geneva Convention III.

**International law and the war on terrorism.** After the September 11 attacks, the United States launched a war on Afghanistan, whose Taliban regime was harboring and abetting operatives of the al-Qaeda terror network. The United States transported large numbers of Taliban and al-Qaeda personnel to holding centers at Guantanamo Bay, U.S.-controlled territory on the island of Cuba. U.S.

authorities accorded Taliban members, because they represented a national government, the rights of POWs, but regarded al-Qaeda personnel as mercenaries according to international law.

In practice, this distinction resulted in more aggressive questioning, and less concern for the physical comfort, of al-Qaeda operatives. Nevertheless, al-Qaeda personnel were provided with basic necessities, allowed to practice their religion, and otherwise treated in a manner no different from their Taliban cohorts. However, many groups in Europe and America regarded the distinction between al-Qaeda and Taliban as unlawful, and the American Bar Association passed a resolution calling for the granting of legal counsel to al-Qaeda detainees. Many critics of American policy cited "Protocol One," a 1977 addition to the Geneva Conventions designed to provide rights to personnel previously regarded as "unlawful combatants." President Ronald Reagan had rejected "Protocol One" in 1987 on the grounds that it was designed to protect the rights of terrorists.

American actions against terrorists also elicited criticism when senior al-Qaeda operative Khaled Sheikh Mohammed, captured in Pakistan in 2003, was detained in an undisclosed location while U.S. personnel—in the words of a Department of Defense statement—applied "all appropriate pressure" to extract intelligence from him. Government officials maintained repeatedly that Mohammed was not being tortured, and several noted that, aside from all moral or legal implications, torture is not usually an effective means of obtaining reliable information.

#### ■ FURTHER READING:

##### BOOKS:

- Kish, John, and David Turns. *International Law and Espionage*. Boston: M. Nijhoff Publishers, 1995.
- Reisman, W. Michael, and James E. Baker. *Regulating Covert Action: Practices, Contexts, and Policies of Covert Coercion Abroad in International and American Law*. New Haven, CT: Yale University Press, 1992.

##### PERIODICALS:

- Bonner, Raymond, et al. "Questioning Terror Suspects in a Dark and Surreal World." *New York Times*. (March 9, 2003): 1.
- Bowman, M. E. "Intelligence and International Law." *International Journal of Intelligence and Counterintelligence* 8, no. 3 (fall 1995): 321–335.
- Khor, Jennifer. "Information Gathering, the Law of War, and Peacekeeping." *Peacekeeping & International Relations* 24, no. 6 (November 1995): 16.
- McManus, Doyle. "A U.S. License to Kill." *Los Angeles Times*. (January 11, 2003): A1.
- Rivkin, David B., Jr. "The Laws of War." *Wall Street Journal*. (March 4, 2003): A14.

##### SEE ALSO

*CIA, Legal Restriction*

*Electronic Communication Intercepts, Legal Issues*  
*Interpol (International Criminal Police Organization)*  
*Interrogation: Torture Techniques and Technologies*  
*Privacy: Legal and Ethical Issues*  
*Telephone Recording Laws*

## Intelligence and Law Enforcement Agencies

■ JUDSON KNIGHT

Despite the obvious relationship between intelligence and law enforcement, historically a number of barriers have separated the two. One of the most important of those barriers in the American experience has been the law itself, which has sought to prevent the development of an internal security apparatus more suited to an authoritarian or totalitarian nation than a liberal democracy. The end of the Cold War and the subsequent war on terrorism, however, presented the nation with threats that seemed to require blurring the lines between intelligence and law enforcement. These changes have in turn forced a rethinking of the relationship between national security, internal security, and the rights of citizens under the rule of law.

**“Posse Comitatus” law.** Few ideas are as antithetical to American sensibilities as the notion of a government free to enforce its will with armed troops, or invisible spies, moving among the citizenry. Only once in American history has martial law prevailed over a large geographic region for an extensive period. That period was the Reconstruction (1865–77), in which the former states of the Confederacy were ruled by federal troops. In the aftermath of the Reconstruction, Congress passed the Posse Comitatus Act of 1878. The title of the act harkened to an ancient institution of English law whereby the local lord could raise a citizen militia to maintain public order, but the purpose of the 1878 law was to protect the citizenry from encroachments by government.

Although the Posse Comitatus Act made it illegal to use the U.S. military to enforce domestic law, a few occasions in the years since have necessitated adjustments. Such was the case in 1957, for instance, when President Dwight D. Eisenhower federalized the Arkansas National Guard and used it, along with the 101st Airborne Division, to integrate the high schools of Little Rock, Arkansas. Again in the 1980s, President Ronald Reagan used the military for the domestic “war on drugs.”

**Restrictions on the intelligence community.** The National Security Act of 1947, which created the Central Intelligence Agency (CIA), explicitly forbade it from operating in

a law-enforcement or internal security capacity. With World War II recently concluded, America’s leaders had a negative example in the form of the Nazis’ Gestapo, not to mention the Soviet internal security apparatus that would become the KGB in the 1950s. Additionally, the National Security Act reinforced a division of labor between the nascent intelligence community (represented during the war by the Office of Strategic Services, or OSS) and the highest law-enforcement agency in the land, the Federal Bureau of Investigation (FBI). Though the FBI had been engaged in intelligence-gathering operations in Latin America, for the most part it had maintained its focus on internal affairs while OSS concentrated on external ones.

In today’s U.S. intelligence community, which consists of more than a dozen agencies, most are members of the Department of Defense (DOD), which is effectively prevented by posse comitatus law from playing a role in internal security. Another factor that discourages the blurring of law enforcement and intelligence is the strong sentiment against domestic intelligence and surveillance operations such as those conducted by the FBI under the leadership of J. Edgar Hoover in the 1950s and 1960s. Such activities, when they came to light, served to reinforce a growing attitude of suspicion toward the federal government.

**New threats and the blurring of lines.** Countering popular concerns for civil liberties and the rule of law are growing threats to national and internal security whose response almost seems to necessitate a blurring between intelligence and law enforcement duties. This has been particularly the case with the end of the Cold War and the rise of terrorist organizations. Not only do the latter threaten national security, but they are also involved in a number of activities usually dealt with by law enforcement: drug trafficking, counterfeiting, money laundering, and so on.

Additionally, the 1990s saw the rise of internal terrorism such as that perpetrated by the Oklahoma City bombers and the Unabomber. These actions required a response by domestic law-enforcement agencies, including the FBI and the Bureau of Alcohol, Tobacco, and Firearms. In a move that resembled actions of the CIA or National Security Agency, the FBI reportedly used satellites to conduct surveillance on Theodore Kaczynski, the Unabomber.

This new environment of combined law enforcement and intelligence efforts was reflected by the rise of state and local organizations devoted to providing intelligence to law enforcement agencies. An example was the Intelligence Network of the Iowa Department of Safety, established in 1984 to support multi-jurisdictional operations within the state. Law enforcement agencies in the Washington, D.C., and Baltimore area formed the Washington-Baltimore High Intensity Drug Trafficking Area Information Center, designed to serve as a hub for intelligence on drug and weapons trafficking, as well as money laundering, in the two cities.



As early as March, 1993, an awareness of the potential problems to be faced by the increased merging of law enforcement and intelligence operations spurred the formation of a federal study panel. In August, 1994, the Joint Task Force on Intelligence and Law Enforcement released a series of recommendations, including the creation of "focal points," or coordinating offices, that would provide an interface between the Justice Department and CIA. A decade later, the FBI and CIA engaged in a turf battle over new domestic intelligence responsibilities that arose from the war on terror. The administration of President George W. Bush chose to make CIA the lead agency in those efforts.

#### ■ FURTHER READING:

##### BOOKS:

Best, Richard A., Jr. *Intelligence and Law Enforcement: Countering Transnational Threats to the U.S.* Washington, D.C.: Congressional Research Service, 2001.

##### PERIODICALS:

EGGEN, DAN. "FBI Seeks Data on Foreign Students; College Calls Request Illegal." *Washington Post*. (December 25, 2002): A1.

PHILLIPS, EDWARD H. "It Wasn't Us." *Aviation Week & Space Technology* 144, no. 15 (April 8, 1996): 19.

##### ELECTRONIC:

Information Center. Washington-Baltimore High Intensity Drug Trafficking Area. <[http://www.hidta.org/programs/info\\_center.asp](http://www.hidta.org/programs/info_center.asp)> (April 4, 2003).

Iowa Law Enforcement Intelligence Network. <<http://www.state.ia.us/government/dps/intell/support.htm>> (April 4, 2003).

##### SEE ALSO

*CIA, Legal Restriction*  
*Crime Prevention, Intelligence Agencies*  
*DEA (Drug Enforcement Administration)*  
*Domestic Intelligence*  
*Drug Intelligence Estimates*  
*Intelligence Community*  
*Law Enforcement, Responses to Terrorism*

---

## Intelligence & Research (INR), United States Bureau of

---

The Bureau of Intelligence & Research (INR) is a unit of the U.S. State Department tasked with providing intelligence to department policymakers. As the major State Department component of the U.S. intelligence community, it

holds a unique position, as most intelligence organizations are affiliated, either directly or by association, with the Department of Defense (DOD). In addition to its intelligence work, INR is involved in a number of geographic issues, from studying boundaries to encouraging geographic learning among U.S. students.

Established in 1946, INR assists the Secretary of State with timely assessments of international events through value-added independent analysis. It is the job of INR to ensure that intelligence activities support not only national security purposes (traditionally the topmost priority of DOD) but also foreign policy, a much greater concern for State. Although its principal customer is the State Department, INR also supplies its services to the White House, National Security Council, DOD, and other agencies within the intelligence community.

The 19 offices of INR are a reflection of the geographic and functional bureaus within the Department of State. INR employs some 300 persons, of whom about 75 percent are members of the civil service, with the remainder from the Foreign Service. These personnel speak and/or read a total of 36 languages, and 71 percent have post-graduate degrees. The average INR analyst has spent 13 years studying the country in which he or she is tasked. In addition to monitoring incoming traffic, INR analysts continually work to integrate data and insights into their ongoing analysis of overseas situations.

Additionally, INR has specialists concerned with analyzing international boundary issues and disputes. With its emphasis on geographic learning, INR has been a leading proponent of geography education for American students. On the Internet, it maintains its Geographic Learning Site for students from kindergarten through high school.

#### ■ FURTHER READING:

##### BOOKS:

*Global Trends 2015: A Dialogue about the Future with Nongovernment Experts.* Langley, CA: National Intelligence Council, 2000.

*INR, Intelligence and Research in the Department of State.* Washington, D.C.: Bureau of Intelligence and Research, 1983.

##### PERIODICALS:

BARNES, SCOTTIE. "State Department Hosts Forum on Geographic Information." *Geospatial Solutions* 12, no. 9 (September 2002): 18.

MEYER, JOSH. "At Least 70,000 Terrorist Suspects on Watch List." *Los Angeles Times*. (September 22, 2002): A1.

##### ELECTRONIC:

Bureau of Intelligence and Research. U.S. Department of State. <<http://www.state.gov/s/inr/>> (April 7, 2003).

Department of State. U.S. Intelligence Community. <[http://www.intelligence.gov/1-members\\_state.shtml](http://www.intelligence.gov/1-members_state.shtml)> (April 7, 2003).

## SEE ALSO

*Department of State, United States Intelligence Community Terrorist Organization List, United States*

## Intelligence Authorization Acts, United States Congress

Intelligence authorization acts are annual legislative Acts of Congress whereby current intelligence issues are addressed and appropriations made for intelligence activities in the coming year. These date to 1979, although the first true intelligence authorization act was signed by President Ronald Reagan in 1981. The intelligence authorization acts are an example of the increased legislative oversight of intelligence activities that originated in the mid-1970s.

As a result of the Watergate scandal and its implication of the Central Intelligence Agency (CIA) as a participant in some part, combined with numerous revelations of clandestine CIA activities, Congress enacted a number of measures to exert greater legislative control over intelligence activities. Among these was the practice of passing yearly intelligence authorization acts.

The first of these was the Intelligence and Intelligence-Related Activities Authorization Act of 1979. The Act for 1980 had the same title, and only in 1981 was it titled the Intelligence Authorization Act. The 1981 Act was particularly important inasmuch as it established the process whereby the CIA notifies the leadership of the House and Senate intelligence committees of covert actions it intends to undertake.

Intelligence authorization acts have been passed in each fiscal year since 1981. They are far from a “rubber stamp” of the CIA or the administration. For instance, President William J. Clinton vetoed the original Intelligence Authorization Act for Fiscal Year 2001 (H.R. 5630) because of what he called “the badly flawed provision that would have made a felony of unauthorized disclosure of classified information.”

### ■ FURTHER READING:

Bush, George W. “Remarks on Signing the Intelligence Authorization Act for Fiscal Year 2003.” *Weekly Compilation of Presidential Documents* 38, no. 48 (December 2, 2002): 2101–2102.

———. “Statement on Signing the Intelligence Authorization Act for Fiscal Year 2002.” *Weekly Compilation of Presidential Documents* 37, no. 52 (December 31, 2001): 1834.

Cannon, Carl M. “Central Intelligence Agency.” *National Journal* 33, no. 25 (June 23, 2001): 1903–1904.

Clinton, William J. “Statement on Signing the Intelligence Authorization Act for Fiscal Year 2001.” *Weekly Compilation of Presidential Documents* 36, no. 52 (January 1, 2001): 3184–3185.

## SEE ALSO

*Bush Administration (1989–1993), United States National Security Policy*

*Bush Administration (2001–), United States National Security Policy*

*CIA, Legal Restriction*

*Clinton Administration (1993–2001), United States National Security Policy*

*Intelligence, United States Congressional Oversight President of the United States (Executive Command and Control of Intelligence Agencies)*

*Reagan Administration (1981–1989), United States National Security Policy*

## Intelligence Community

The United States Intelligence Community (IC) is a group of 14 agencies and organizations responsible for conducting intelligence activities necessary to the national security of the United States and the success of its foreign relations. Headed by the Director of Central Intelligence (DCI), its members include the Central Intelligence Agency (CIA), a number of Department of Defense (DOD) agencies and organizations, and intelligence-gathering agencies within the departments of State, Energy, Justice, the Treasury, and Homeland Security.

### Defining the Intelligence Community

In contrast to the generic term “intelligence community,” the United States has a formal Intelligence Community established as a result of Executive Order 12333, signed by President Ronald Reagan on December 4, 1981. The order directs, in part, that the United States intelligence effort shall provide the president and the National Security Council with the necessary information on which to base decisions concerning the conduct and development of foreign, defense, and economic policy, and the protection of United States national interests from foreign security threats. All departments and agencies shall cooperate fully to fulfill this goal.

In addition to the CIA, the IC includes 13 other agencies and organizations. Those from DOD include the Defense Intelligence Agency (DIA), National Security Agency (NSA), National Reconnaissance Office (NRO),



(l to r) Former U.S. Attorney Mary Jo White, former Senator Warren Rudman, former FBI director Louis Freeh, and CIA National Intelligence Officer Paul Pillar are sworn in during intelligence hearings, 2002. AP/WIDE WORLD PHOTOS.

National Imagery and Mapping Agency (NIMA), and the intelligence agencies of the Army, Navy, Air Force, and Marine Corps. Non-DOD members include the Federal Bureau of Investigation (a part of the Justice Department), the United States Coast Guard (part of the Department of Homeland Security as of 2003), the State Department's Bureau of Intelligence and Research, and the intelligence agencies of the Energy and Treasury departments.

## Tasks

The 14 members of the IC work separately and together in fulfillment of a number of functions. They collect information required by the president, the National Security Council (NSC), the secretaries of state and defense, and other officials of the executive branch. In meeting the needs of these and other customers, they produce and disseminate a variety of intelligence gathered through the four traditional methods of intelligence collection: human, signals, imagery, and measurement and signatures intelligence (HUMINT, SIGINT, IMINT, and MASINT respectively).

Intelligence collection is directed toward information on international terrorist and narcotics trafficking activities, as well as other hostile activities against the United States by foreign powers, organizations, persons, and/or their agents. Members of the IC are also involved in the

conduct of special activities, which can and do involve covert action against entities deemed a threat to national security.

**Leadership and oversight.** The DCI serves a triple function as head of the CIA, principal intelligence advisor to the president, and director of the IC. He reports to the president, directly and through the national security advisor and/or the NSC. Each year, DCI presents the president with the annual IC budget, known as the National Foreign Intelligence Program (NFIP).

As head of the IC, the DCI is responsible for directing and coordinating national foreign intelligence activities, though he only exercises direct authority over CIA, as well as staff organizations outside the CIA. The latter include the National Intelligence Council (NIC), responsible for preparing national intelligence estimates, and the Community Management Staff, which assists DCI in his IC executive functions.

**Advisory boards.** DCI also chairs two advisory boards, the National Foreign Intelligence Board (NFIB) and the Intelligence Community Executive Committee (IC/EXCOM). Membership of both is made up of representatives from IC agencies. The NFIB exercises authority over approving

national intelligence estimates, coordination of interagency intelligence exchanges as well as exchanges with the intelligence and security agencies of friendly foreign nations, and development of policy for the protection of intelligence sources and methods.

The IC/EXCOM advises DCI on national intelligence policy and resource issues, including matters relating to the IC budget, the establishment of needs and priorities, evaluation of intelligence activities, and formulation and implementation of intelligence policy. Its members include, in addition to DCI, the Deputy Secretary of Defense and undersecretaries whose roles relate to intelligence; the Vice Chairman of the Joint Chiefs of Staff; the directors of NSA, NRO, NIMA, and DIA; the Assistant Secretary of State for Intelligence and Research; the NIC chairman; and the executive directors for IC affairs and CIA.

**Internal and external oversight.** A number of mechanisms exist for providing oversight and accountability to the IC. These include entities within its membership, as well as from both the executive and legislative branches of government. Within the IC is the CIA Inspector General, appointed by the President and confirmed by the Senate, who is responsible for investigating allegations of impropriety and mismanagement within CIA. DOD has its own inspector general, a position created by statute, while DOD elements of the IC have non-statutory inspectors general appointed by the directors of the respective agencies. Independent inspectors general exert oversight for non-DOD member organizations.

At the executive level, the Intelligence Oversight Board of the President's Foreign Intelligence Advisory Board provides oversight, and reviews the functions of IC oversight mechanisms. In the area of budgeting, controlled ultimately by the President, the Office of Management and Budget ensures that IC activities comport with the President's overall program. Within the executive branch, Congress provides checks and balances through the Senate Select Committee on Intelligence, the House Permanent Select Committee on Intelligence, and other committees concerned with activities relating to national security.

#### ■ FURTHER READING :

##### BOOKS:

- Fain, Tyrus G., and Katharine C. Plant. *The Intelligence Community: History, Organization, and Issues*. New York: R. R. Bowker, 1977.
- Gore, Albert. *The Intelligence Community: Accompanying Report of the National Performance Review, Office of the Vice President*. Washington, D.C.: U.S. Government Printing Office, 1993.
- Hopple, Gerald W., and Bruce W. Watson. *The Military Intelligence Community*. Boulder, CO: Westview Press, 1986.
- Kirkpatrick, Lyman B. *The U.S. Intelligence Community: Foreign Policy and Domestic Activities*. New York: Hill and Wang, 1973.

Richelson, Jeffrey T. *The U.S. Intelligence Community*, fourth edition. Boulder, CO: Westview Press, 1999.

Smist, Frank John. *Congress Oversees the United States Intelligence Community, 1947–1989*. Knoxville: University of Tennessee Press, 1990.

#### ELECTRONIC:

- Intelligence Agency Profiles. Federation of American Scientists. <<http://www.fas.org/irp/agency/>> (April 14, 2003).
- U.S. Intelligence Community. <<http://www.intelligence.gov/>> (April 14, 2003).

#### SEE ALSO

- Air Force Intelligence, United States*  
*CIA (United States Central Intelligence Agency)*  
*Coast Guard (USCG), United States*  
*DCI (Director of the Central Intelligence Agency)*  
*DIA (Defense Intelligence Agency)*  
*DOD (United States Department of Defense)*  
*DOE (United States Department of Energy)*  
*FBI (United States Federal Bureau of Investigation)*  
*INSCOM (United States Army Intelligence and Security Command)*  
*Intelligence & Research (INR), United States Bureau*  
*Intelligence, United States Congressional Oversight*  
*NIC (National Intelligence Council)*  
*NSC (National Security Council)*  
*NFIB (United States National Foreign Intelligence Board)*  
*NIMA (National Imagery and Mapping Agency)*  
*NMIC (National Maritime Intelligence Center)*  
*NRO (National Reconnaissance Office)*  
*NSA (United States National Security Agency)*  
*PFIAB (President's Foreign Intelligence Advisory Board)*  
*President of the United States (Executive Command and Control of Intelligence Agencies)*  
*Treasury Department, United States*

---

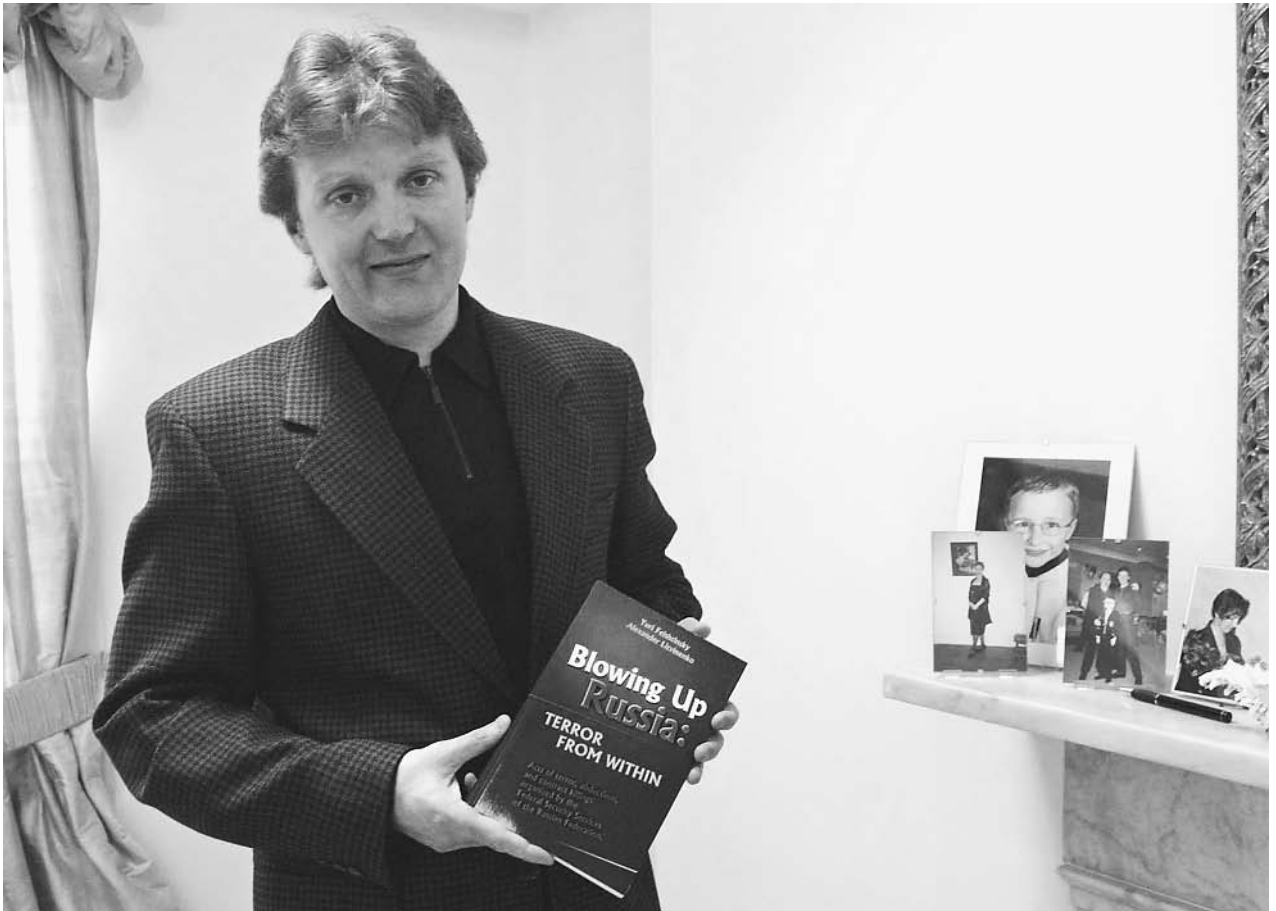
## Intelligence Literature

---

#### ■ TABITHA SPARKS

The emergence of the "spy thriller" in the twentieth century reflects the modern era's technological advancements, and the institutionalization of intelligence services that works to monitor these advancements and their attendant risks on the global stage. Political conflicts between nations are the staple feature of the literature of espionage or intelligence, which also usually figures a heroic spy at the center of the international crisis. While spy novels for most of the twentieth century were dominantly a British invention, American novelists in the last decades have contended for the audience of this hugely popular genre.

The genre of the British spy novel that exploded in the early twentieth century has many nineteenth century influences. The global expansion of the British Empire in the second half of the nineteenth century introduced into



Alexander Litvinenko, former KGB spy and author of the book *Blowing Up Russia: Terror from Within*, photographed at his home in London in 2002. While serving in Russia's main security agency, Litvinenko's job was to try to infiltrate and topple terrorist networks. AP/WIDE WORLD PHOTOS.

British culture a range of foreign interests, languages, and customs. British power faltered as the nation expanded into colonies, inciting fears about the loss of British identity in the face of rapid foreign expansion. Many late-Victorian novels pit blameless Englishmen and women against evil foreigners in a black-and-white interpretation of the threats to "home" from abroad. The heightened sense of xenophobia was one precursor to the spy genre that rested upon the security of national borders.

Early British novels that feature the threat of imperial invasion and/or power include Bram Stoker's *Dracula* (1898) and Rudyard Kipling's *Kim* (1901). While not formally a spy novel, *Dracula* contains a detailed international plot whereby the title character, a vampire, is finally ensnared by a band of heroic Englishmen. Kipling's novel takes place in India, with an Anglo-Indian boy using his ambiguous racial identity as a cover for colonial espionage, or the "Great Game" between European and Asian factions.

Alongside a growing awareness of an increasingly pluralistic world was a rise of technology that made national security and police work a modern science. Fascination with detective work and forensics at the end of the

nineteenth century is exemplified by popular interest in the Jack-the-Ripper murders in London (the 1880s and 90s), and Arthur Conan-Doyle's series of detective novels featuring Sherlock Holmes. Both murder case and detective series detailed the new technologies of modern police work, including fingerprinting, handwriting analysis, and instruments of surveillance such as the camera and the telescope.

Joseph Conrad's critically acclaimed novels include several tales of espionage. *The Secret Agent* (1907) and *Under Western Eyes* (1911) critique the autocratic and revolutionary regimes in a stunning anticipation of World War I and the Bolshevik Revolution of 1917. The psychological complexity of Conrad's novels set them apart from the new wave "spy thrillers" written during this period, which predominantly depend on action and suspense rather than interior character development.

The spy novel in the early twentieth century was inspired most specifically by the advent of organized intelligence agencies in the period prior to World War I. The expansion of the London publishing industry in the late 1800s and early 1900s also contributed to the growing market for "pot boilers"—novels including spy thrillers

with popular appeal but little critical value. These books are formulaic, usually with simplistically drawn good and evil characters, but appealed for their seemingly topical reflection of current politics.

Erskine Childers's *The Riddle of the Sands* (1903), for instance, concerns two Englishmen uncovering a German plot to launch a naval attack on Great Britain. The novel was so convincing in its analysis of naval security that the British Naval Intelligence Division was moved to investigate Childers himself for possible underground associations.

Among the many anti-German spy novels in English during this period are best-selling author William LeQueux's *Spies of Kaiser* (1909), which includes exhaustive descriptions of technological gadgetry of the new age of espionage, and E. Phillips Oppenheim's *The Kingdom of the Blind* (1916). Oppenheim's novel built upon the anti-German sentiment following the German sinking of the British ship *The Lusitania* in 1915, and includes a plot to sink a passenger ship. Also enormously popular was John Buchan's *The Thirty-Nine Steps* (1915), which details the urgent necessity for counterespionage in a typical German plot against the English navy.

Following World War I and the cynicism it fostered, the next phase of espionage literature reflects a perspective increasingly critical of official state authority. The spies in works by authors including Eric Ambler, Somerset Maugham, and especially, Graham Greene, often are lonely individuals on the outskirts of a power-hungry or opportunistic state government. Maugham and Greene built their reputations in part upon their own experience in espionage. During the Russian Revolution of 1917, Maugham went under cover as a reporter in order to communicate information to British Intelligence. While his novels and stories do not exclusively focus on espionage, he is credited with writing the first modern spy story with literary merit. This work is *Ashenden; or the British Agent* (1928), inspired by his own experience in Russia, and more famously known through Alfred Hitchcock's film interpretation, *The Secret Agent*.

Greene worked with the British Secret Intelligence Service in Sierra Leone (1941), a job he found perfunctory. His critique of the Intelligence Service emerges in left-wing novels, from *The Quiet American* (1952) and *A Burnt-out Case* (1961), to *The Human Factor* (1978).

Writing spy fiction at the same time as Greene, but in a very different style was Ian Fleming, the creator of Britain's most famous fictional spy, James Bond. Fleming, like Greene, had also worked as a spy, but his far-fetched and spectacular plots (which depend heavily on fantastic gadgetry and amazing escapes) appeal to an audience more interested in sensation than realism. Some of Fleming's most famous tales (many of which have been made into movies) include *Dr. No* (1958) and *Goldfinger* (1959), which figure Chinese and Russian threats to Western capitalism.

Challenging Bond's flashy exploits are the fictional spies created by British authors John le Carré and Len Deighton. These writers stress the moral conflicts inherent in espionage and geopolitical conflict, particularly during the Cold War. For instance, in le Carré's *The Spy Who Came in from the Cold* (1963), the hero himself ultimately dies on the Berlin Wall, after infiltrating East German intelligence. Le Carré's *The Tailor of Panama* (1966) and Deighton's *The Ipcress File* (1962) concern internal corruption of the intelligence service; their spies face crimes from both inside and outside their governments and bureaucracies.

British dominance in espionage literature waned somewhat during the last quarter of the twentieth century. Since the 1980s, American novelists including Robert Ludlow and Tom Clancy have rivaled their British counterparts in writing best-selling spy fiction. Clancy's hero Jack Ryan foils Cold War plots in novels including *The Hunt for Red October* (1984) and *Patriot Games* (1987), from a pro-government, relatively conservative vantage point. These stories have become popular films, with their emphasis on technology and gadgetry translating easily to the visual medium.

A somewhat ambivalent treatment of the security services, such as those offered by the nuanced works of le Carré and Deighton, perhaps anticipates the future of the literature of intelligence. The world of international politics is no longer viewed as Western-centric or bipolar (divided into adversarial nation states) as it was throughout much of the twentieth century. As international secret services turn to current crises like drug trafficking and bioterrorism, the shrinking world stage will likely be reflected on the pages of the literature of intelligence in the coming generations.

#### ■ FURTHER READING:

##### BOOKS:

- Cawalti, John G., and Bruce A. Rosenberg. *The Spy Story*. Chicago: University of Chicago Press, 1987.
- Panek, LeRoy L. *The Special Branch: The British Spy Novel, 1890–1980*. Bowling Green, Ohio: Bowling Green University Popular Press, 1981.
- Smith, Myron J., Jr., and Terry White. *Cloak and Dagger Fiction: An Annotated Guide to Spy Thrillers*, 3rd ed. New York: Greenwood Press, 1995.
- Winks, Robin W. (ed. and introd.); Maureen Corrigan (ed.) *The Literature of Crime, Detection, and Espionage, I–II*. New York: Charles Scribners, 1998.

##### PERIODICALS:

- Price, Thomas J. "Spy Stories: Espionage and the Public in the Twentieth Century." *Journal of Popular Culture* no. 30 (1996): 81–89.

##### SEE ALSO

*Cold War (1945–1950): The Start of the Atomic Age*

*Cold War (1950–1972)*  
*Cold War (1972–1989): The Collapse of the Soviet Union*  
*Great Game*

## Intelligence Officer

An intelligence officer is a professional employed by an intelligence service. Members of the intelligence community make sharp distinctions between intelligence officers and intelligence agents, who are outsiders employed by the intelligence agency. Intelligence officers, on the other hand, are operatives of the agency itself, but their professional role—and the fact that many are military officers and/or intelligence specialists—gives them particular distinction.

The distinction goes back to World War II and the origins of modern intelligence agencies. At that time, Office of Strategic Services (OSS) manuals defined an operative as “an individual employed by and responsible to the OSS and assigned under special programs to field activity.” An agent, on the other hand, was defined by OSS as “an individual recruited in the field who is employed or directed by an OSS operative.” The Central Intelligence Agency (CIA), successor to OSS, calls its operatives CIA officers.

Intelligence officers often work with agents in the role of case officer. A case officer is an intelligence officer whose job it is to supervise agents working on a case, a term referring to an entire intelligence operation. The case officer provides direction to the agent, and if the case officer works on a one-on-one basis with the agent, then he or she is known as the agent’s handler. An intelligence officer may assign one agent to perform the role of surrogate handler, working directly with other agents and reporting to the intelligence officer. In that case, the surrogate handler is known as a principal agent.

### ■ FURTHER READING:

#### BOOKS:

- Phillips, David Atlee. *Careers in Secret Operations: How to Be a Federal Intelligence Officer*. Frederick, MD: University Publications of America, 1984.
- Roosevelt, Archibald. *For Lust of Knowing: Memoirs of an Intelligence Officer*. Boston: Little, Brown, 1988.
- Wright, Peter. *Spycatcher: The Candid Autobiography of a Senior Intelligence Officer*. New York: Viking, 1987.
- Zacharias, Ellis M. *Secret Missions: The Story of an Intelligence Officer*. New York: G. P. Putnam’s Sons, 1946.

#### SEE ALSO

*Intelligence*  
*Intelligence Agent*  
*Intelligence and Counter-Espionage Careers*

## Intelligence Policy and Review (OIPR), United States Office of

The Office of Intelligence Policy and Review (OIPR) advises the United States attorney general regarding matters relating to U.S. national security activities. In accordance with the Foreign Intelligence Surveillance Act of 1978, OIPR prepares and files all applications for authorization to conduct electronic surveillance and physical searches. It also acts as legal adviser, not only to the attorney general and the Department of Justice as a whole, but also to the Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), Department of Defense, Department of State, and other federal agencies. Additionally, OIPR acts as the Department of Justice representative on several interagency committees.

Acting under the direction of the Counsel for Intelligence Policy, the attorney general’s legal adviser in intelligence matters, OIPR helps keep the attorney general—as the chief law-enforcement executive in the United States—abreast of all relevant national security activities. Under the provisions of the Foreign Intelligence and Surveillance Act, OIPR also prepares applications for surveillance and searches, and presents these to the U.S. Foreign Intelligence Surveillance Court.

Both for the attorney general and for various intelligence agencies such as the CIA, OIPR provides formal and informal legal counsel on matters relating to U.S. intelligence activities and procedures. For example, in the 1980s, OIPR helped bring an end to an FBI probe of the Committee in Support of the People of El Salvador (CISPES). That group supported the overthrow of the Salvadoran government by Marxist guerrillas, but based on OIPR’s analysis, did not appear to be a communist front organization, and OIPR advised FBI leadership in 1985 that the probe threatened CISPES’s First Amendment rights.

More than a decade later, OIPR was involved in the scandals surrounding Chinese nuclear spying in the United States during the administration of President William J. Clinton. OIPR twice received applications to wiretap scientist Wen Ho Lee at the Los Alamos National Laboratory, and twice rejected these applications on the basis that there was not sufficient evidence against him. The FBI disagreed, and in 1999, Attorney General Janet Reno blamed the burgeoning scandal in part on the two agencies for not bringing their disagreement before her.

OIPR serves as a sounding board for other agencies’ opinions on matters involving proposed legislation regarding intelligence-related matters. It also represents the attorney general on a variety of interagency task forces and committees concerned with issues of national security and nonproliferation, as well as scientific exchanges,

administration of exports, information security, personnel security, and foreign overflights of U.S. territory. Serving the Department of Justice as a whole, OIPR represents the department on interagency committees, including the National Foreign Intelligence Council.

Within the Justice Department, OIPR heads the Department Review Committee, which carries out department policy on security classifications and makes decisions regarding Privacy Act and Freedom of Information Act appeals. On the Intelligence-Law Enforcement Policy Board, OIPR co-chairs a variety of groups whose purpose is to facilitate better working relationships between components of the intelligence, security, and law-enforcement communities.

## ■ FURTHER READING :

### PERIODICALS:

Jackson, Robert L. "Sessions Concedes FBI Erred in Central American Activist Probe." *Los Angeles Times*. (February 3, 1988): 16.

Safire, William. "Whitewash at Justice." *New York Times*. (July 16, 1999): A19.

### ELECTRONIC:

Office of Intelligence Policy and Review. Department of Justice. <<http://www.usdoj.gov/oipr/>> (March 15, 2003).

Office of Intelligence Policy and Review. Federation of American Scientists. <<http://www.fas.org/irp/agency/doj/oipr/>> (March 15, 2003).

### SEE ALSO

*Chinese Espionage Against the United States*  
*Clinton Administration (1993–2001), United States National Security Policy*  
*Counter-intelligence*  
*FBI (United States Federal Bureau of Investigation)*  
*Foreign Intelligence Surveillance Act*  
*Foreign Intelligence Surveillance Court of Review*  
*Justice Department, United States*  
*Reagan Administration (1981–1989), United States National Security Policy*

---

## Intelligence Support, United States Office of

---

The Office of Intelligence Support (OIS) is the sole United States Treasury Department office that also belongs to the national Intelligence Community. Established in 1977 to replace the Office of National Security, it assists the Secretary of the Treasury, who serves as the president's chief economic and financial adviser as well as the head of the

second largest federal law-enforcement department. The OIS also participates in the preparation of National Intelligence Estimates.

In 1961, Treasury Secretary Douglas Dillon established the Office of National Security (ONS) to act as an interface, liaison, and coordinator between Treasury and the National Security Council. Ten years later, in 1971, a presidential memorandum clearly established the ONS as a member of the U.S. Intelligence Community. In response to the report of the Murphy Commission to Congress, which placed an emphasis on links between the Intelligence Community and the nation's economic policy leadership, Treasury was added to the National Foreign Intelligence Board in 1972.

In 1977, Treasury Secretary Michael Blumenthal changed ONS to OIS to emphasize its role in support of the Intelligence Community. Executive Order 12333 ("United States Intelligence Activities"), issued by President Ronald Reagan on December 4, 1981, explicitly spelled out the intelligence role of Treasury alongside that of other agencies and departments more obviously connected with intelligence gathering. The Special Assistant to the Secretary (National Security) is a senior officer in the Intelligence Community, as noted in E.O. 12333. On December 19, 2002, Treasury Secretary Paul H. O'Neill issued Treasury Order 113-01, defining the duties and responsibilities both of the Special Assistant and the office he or she directs, OIS.

The Special Assistant, along with his or her staff, supports the Secretary of the Treasury, whose critical functions include his or her role as chief economic and financial adviser to the president; director of the second-largest department in the federal government (after Justice) with law-enforcement authority; and chief official responsible for the integrity of U.S. currency. The Special Assistant is charged by 113-01 with providing day-to-day intelligence support to the Secretary and other officials, representing Treasury on committees of the Intelligence Community, and maintaining continuous liaison between Treasury and members of that community.

There are three principal components to the mission of OIS. First, it is responsible for alerting the Secretary and other officials of fast-breaking events, both foreign and domestic, of which it becomes aware as chief intelligence officer of the treasury. Second, it provides Treasury officials with intelligence reports and products, usually obtained from Intelligence Community collectors and producers of intelligence. Finally, it is charged with overseeing the relationship between Treasury's offices and bureaus and the members of the Intelligence Community, as well as the Community as a whole.

Additionally, OIS assists in the preparation of National Intelligence Estimates. It also assists other members of the Intelligence Community in the production of intelligence by contributing information to which Treasury is privy. OIS officers act as Treasury representatives of national



intelligence committees and subcommittees within the Intelligence Community.

#### ■ FURTHER READING :

##### ELECTRONIC:

Office of Intelligence Support. Federation of American Scientists. <<http://www.fa.org/irp/agency/ustreas/tdois.htm>> (March 17, 2003).

U.S. Department of the Treasury. <<http://www.ustreas.gov>> (March 17, 2003).

##### SEE ALSO

*Intelligence Community*  
*National Intelligence Estimate*  
*NFIB (United States National Foreign Intelligence Board)*  
*Treasury Department, United States*

## Intelligence, United States Congressional Oversight of

#### ■ JUDSON KNIGHT

Although the United States Congress served as facilitator to the establishment of the U.S. intelligence community by passing the National Security Act of 1947, during the next quarter-century it exerted little oversight in matters of intelligence. Then, in the 1970s, as distrust of the executive branch grew in the wake of the Watergate scandal and the Vietnam War, Congress began to take a more activist stance. The result was the formation of the Church Committee in the Senate and the Pike Committee in the House of Representatives, both precursors to permanent committees exerting legislative oversight for intelligence activities. From 1981 onward, presidents have been required to sign Intelligence Authorization Acts, annual requests for funds and authority to undertake broadly defined actions.

For the first quarter-century after it passed the National Security Act, which, among other things, created the Central Intelligence Agency (CIA), Congress had little to say about the activities of the nascent intelligence community. Among significant legislation during this time were the 1949 revisions to the 1947 Act, whereby the structure of the National Security Council was altered; the State Department Basic Authorities Act of 1956; and the National Security Agency Act of 1959. The second of these acts provided rewards leading to the arrest of foreign saboteurs (it was amended to increase the rewards after the September, 2001, terrorist attacks), while the third act formalized aspects of the National Security Agency (NSA)

created in a secret 1952 memorandum by President Harry S. Truman.

The new era of congressional oversight began in 1974, with the passage of the Hughes-Ryan Act amending the Foreign Service Act. Passed in the wake of covert activities that helped bring down the Marxist regime of Salvador Allende in Chile, the Hughes-Ryan Act required the President to submit plans for covert actions to the relevant congressional committees.

The mid-1970s also saw new legislation designed to protect private citizens from government snooping. Congress had passed the Freedom of Information Act (FOIA) in 1967, but strengthened it in 1975 with new provisions that gave U.S. citizens access to files on them kept by federal law-enforcement agencies. In the meantime, the Privacy Act of 1974 greatly restricted the authority of agencies to collect information on individuals, and to disclose that information to persons other than the individual.

**The Church and Pike committees.** In the meantime, the Church Committee (officially known as the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities) had begun meeting in 1975. Its principal focus was domestic intelligence activities, but after interviewing NSA witnesses, it broadened its efforts. Chaired by Frank Church (D-ID), the committee revealed so much about U.S. covert operations that President Gerald R. Ford finally called Church and asked him, in the name of national security, to stop the release of sensitive information.

The Church Committee issued its final report on April 26, 1976, but its effect would extend over several decades. Less well known than the Church Committee was its House counterpart, the Pike Committee. Chaired by Otis Pike (D-NY), it also operated from 1975 to 1976, and likewise focused on the NSA. When Pike demanded a copy of the "charter" establishing NSA, he was rebuffed, as the so-called charter was actually Truman's secret memorandum. Although the committee subpoenaed the directive, the NSA, with help from the Justice Department and the Pentagon, successfully blocked them from seeing it. Aside from a very small portion (revealed only for the purpose of showing that NSA was exempt from certain legal restrictions on the use of communications intelligence), the NSA "charter" remains one of the most deeply buried secrets of the federal government.

Notwithstanding Church's and Pike's partisanship and desire to grandstand, their committees did introduce checks upon the perceived adventurism of the CIA, NSA, and other agencies. These efforts continued into the early 1980s. In 1980, Congress passed the Classified Information Act, which gives guidelines for the use of classified information by both government and defendant in a legal case. A year later, it introduced the Intelligence Authorization Act, whereby the President makes a yearly accounting

of the intelligence community's current and planned operations.

Despite corrective measures that might have established a framework for positive interactions between executive and legislative branches where intelligence was concerned, the 1980s saw a deepening rift between the conservative Republican administration of President Ronald Reagan and the Democrat-dominated Congress. The situation reached its nadir with the Iran-Contra affair, in which the administration and the CIA went around Congress to fund anticommunist fighters in Nicaragua and free American hostages in the Middle East by selling arms to the regime in Iran. Although the Iran-Contra fallout did not result in significant new legislation reaffirming Congressional authority over intelligence activities, the lengthy hearings that followed served to reassert congressional authority.

**Congressional oversight today.** Today, numerous sections of the U.S. Code address intelligence activities, among them Title 5 (Government Organization and Employees), Title 10 (Armed Forces), Title 18 (Crimes and Criminal Procedure), Title 22 (Foreign Relations and Intercourse), and Title 50 (War and National Defense). An annual Intelligence Authorization Act reinforces congressional oversight in the realm of intelligence, as do two standing committees that resulted from the Church and Pike hearings: the Senate Select Committee on Intelligence, and the House Permanent Select Committee on Intelligence.

Congressional authority over intelligence is high, as reflective of a legislative republican democracy under the rule of law. Certainly it will never be high enough for those who subscribe to the conspiratorial view of U.S. intelligence activities; likewise it will always be too high for their counterparts at the other extreme. After the end of Iran-Contra, however, the relationship between Congress, the President, and the intelligence community has been, though far from collegial, usually less than adversarial.

The aftermath of the September, 2001, terrorist attacks, in fact, revealed that national leaders are capable of setting aside differences in the interests of the nation as a whole. In the heightened atmosphere of security that followed those attacks, a growing majority supported a freer rein on intelligence activities. Covert action, minimized as the result of the 1970s and 1980s scandals, would again be on the rise in the fight against terrorism.

#### ■ FURTHER READING:

##### BOOKS:

*Legislative Oversight of Intelligence Activities: The U.S. Experience: Report.* Washington, D.C.: U.S. Government Printing Office, 1994.

Roberts, Brad. *U.S. Foreign Policy After the Cold War.* Cambridge, MA: MIT Press, 1992.

Smist, Frank John. *Congress Oversees the United States Intelligence Community, 1947–1994.* Knoxville: University of Tennessee Press, 1994.

Wittkopf, Eugene R., and James M. McCormick. *The Domestic Sources of American Foreign Policy: Insights and Evidence.* Lanham, MD: Rowman and Littlefield Publishers, 1999.

##### ELECTRONIC:

Intelligence Laws and Regulations. Federation of American Scientists. <<http://www.fas.org/irp/offdocs/laws.htm>> (March 26, 2003).

Intelligence Oversight. <[http://intellinet.muskingum.edu/oversight\\_folder/oversighttoc.html](http://intellinet.muskingum.edu/oversight_folder/oversighttoc.html)> (March 26, 2003).

Sturtevant, Mary. Congressional Oversight of Intelligence: One Perspective. Federation of American Scientists. <<http://www.fas.org/irp/eprint/sturtevant.html>> (March 26, 2003).

##### SEE ALSO

*Church Committee*  
*CIA, Legal Restriction*  
*Classified Information*  
*Electronic Communication Intercepts, Legal Issues*  
*FOIA (Freedom of Information Act)*  
*Intelligence Authorization Acts, United States Congress*  
*Iran-Contra Affair*  
*National Security Act (1947)*  
*President of the United States (Executive Command and Control of Intelligence Agencies)*  
*Privacy: Legal and Ethical Issues*  
*Security Clearance Investigations*  
*Senate Select Committee on Intelligence, United States*

---

## Interagency Security Committee, United States

---

The United States Interagency Security Committee was created on October 19, 1995, by executive order of President Bill Clinton. The order provided for increased security measures for non-military federal buildings. The committee operates within the executive branch of the government and consists of the President and heads of nearly 20 major departments and agencies of the United States government.

After the bombing of the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma, and the first bombing of the World Trade Center in 1993, several government officials lobbied for increased security in and around various federal offices around the nation. While many of the buildings hired private security personnel, or reached agreements with local law enforcement about providing security services, many locations were not adequately

staffed. In addition, some facilities were not built to adequately survive a terrorist attack. The Interagency Security Committee was charged with inspecting each federal facility for structural stability and for needed security measures. The committee further discussed implementation of metal detectors, security cameras, and other security technologies. These measures were intended to create a safer place for people to work.

Other sensitive security needs also fall into the committee's jurisdiction. When the Interagency Security Committee was first assembled, a central database of all federal facilities did not exist. A database was created that not only listed properties, but also building function and condition, security systems, and even employees. This database stores information about the general infrastructure of the extended federal government.

In addition, the creation of the Interagency Security Committee provided increased data protection measures. A number of mishaps involving the loss or mishandling of sensitive information stored on computers prompted the need for centralized discussion of how best to protect federal data. Since the committee's inception, two additional laws have been passed to strengthen computer privacy and data protection not only on the federal, but also on the corporate and private level.

Questions of the overall effectiveness of the committee came into question following the most recent attacks on the World Trade Center and the Pentagon in 2001. Critics claim the database remains incomplete, federal computer privacy systems are dated and ineffective, and overall security in federal facilities has not significantly improved. Others expect the committee to be replaced by or subsumed into the Department of Homeland Security. Many supporters maintain that the committee has not had enough time or resources to finish their task, but have made progress toward their goals.

#### SEE ALSO

*Homeland Security, United States Department of*

## Interception Capabilities.

SEE *ECHELON*.

---

# Internal Revenue Service, United States

---

Among the most visible arms of the U.S. federal government is the Internal Revenue Service (IRS). As most Americans know, the IRS is an office in the Treasury Department

responsible for collecting all individual and corporate taxes. Although dealings with the IRS are sometimes dreaded by taxpayers, it is nevertheless a necessary component of operating the world's only superpower, and the money it collects—more than \$2 billion in 2001—serves to fund operations ranging from the war on terrorism to research into the development of non-petroleum-burning engines. Among the most important components of the IRS is its Criminal Investigation (CI) division, which tracks down tax evaders and helps the federal government in its war on drug trafficking, money laundering, and terrorism.

## History

The history of American taxation is inexorably tied with the history of American military activity. For the better part of a century, the federal government funded its operations through customs tariffs, but in 1862, President Abraham Lincoln created the Office of Internal Revenue to pay expenses associated with the Civil War. A decade later, the income tax was repealed, but it reappeared a half-century later in the beginnings of its modern form, with the ratification of the Sixteenth Amendment to the Constitution in 1913.

The amendment gave Congress the power to levy an income tax, which was collected by the Bureau of Internal Revenue (BIR). The latter had been created in 1877 to collect the few types of taxes that existed at the time, and as America entered World War I, its level of activity increased dramatically. In 1918, the top income tax rate reached a staggering 77 percent, but dropped again to 24 percent in 1929, only to rise again during the Great Depression. The coming of the Second World War brought with it the system of payroll withholding still in place today.

**Formation and Operations.** In 1952, the BIR became the IRS. Up to that time, the agency was staffed by appointees associated with the current presidential administration. Thenceforth, only the IRS commissioner and chief counsel were selected by the President and confirmed by the Senate, with the rest of the IRS run by professionals. Half a century later, the IRS went through a massive program of reform spurred by taxpayer dissatisfaction with the agency, which gained a voice in Washington after Republicans won a majority in Congress in 1994. The result was the IRS Restructuring and Reform Act of 1998, which created provisions to protect taxpayers' rights.

By 2003, the IRS had some 100,000 employees and a budget of \$9.9 billion. It consisted of four major operating divisions: wage and investment, which dealt with 116 million taxpayers who filed individual and joint tax returns; small business and self-employment, which involved some 45 million small businesses and self-employed taxpayers; large and mid-sized business, concerned with corporations possessing assets of more than \$10 million; and tax exempt and government entities, which

also served employee benefit plans. Other areas included the appeals, chief counsel, communications and liaison, and criminal investigation divisions.

**Criminal investigation.** The roots of CI go back to the BIR's Intelligence Unit, created in 1919 and staffed by six U.S. Post Office inspectors. In the 1930s, the unit succeeded in securing the conviction of gangster Al Capone, and assisted in solving the kidnapping of the Lindbergh baby. In July 1978, it assumed its present name. Over the course of its history, CI has had a conviction rate of 90 percent or better, a record unmatched among federal law enforcement agencies.

Staffed by some 2,900 special agents, CI enforces tax and money laundering laws, as well as the Bank Secrecy Act. Its agents are trained in accounting and forensic computer technology, necessary for recovering financial data that may have been encrypted or otherwise hidden by electronic means. In addition to its investigative work, CI serves as an information clearinghouse regarding taxpayer obligations, as well as tax scams. For example, an IRS advisory released in January 2002, warned of slavery reparations scams whereby unscrupulous companies charge African Americans fees to learn how they can receive tax exemption for their ancestors' enslavement. (There is no such exemption.)

The top investigative priorities of CI are legal tax crimes (that is, evasion of taxes on legal income), illegal source financial crimes, and narcotics-related financial crimes. IRS efforts against terrorists fall under the last of these categories, and include operations alongside other federal agencies in a number of multiagency programs such as the Joint Terrorism Task Force and Operation Green Quest. The Strategic Information Operations Center at Federal Bureau of Investigation headquarters in Washington, D.C., coordinates all these efforts.

#### ■ FURTHER READING:

##### BOOKS:

Burnham, David. *A Law unto Itself: Power, Politics, and the IRS*. New York: Random House, 1989.

Davis, Shelley L. *Unbridled Power: Inside the Secret Culture of the IRS*. New York: HarperBusiness, 1997.

##### PERIODICALS:

Leader, Stefan. "Cash for Carnage: Funding the Modern Terrorist." *Jane's Intelligence Review*. (May 1, 1998): 36.

"Victory in the War on Terrorism Will Not Be Won on the Defensive." *New York Times*. (September 10, 2002): A19.

##### ELECTRONIC:

Internal Revenue Service. <<http://www.irs.gov/>> (April 4, 2003).

#### SEE ALSO

ATF (*United States Bureau of Alcohol, Tobacco, and Firearms*)  
Treasury Department, United States

## International Atomic Energy Agency (IAEA)

Established in 1957, the International Atomic Energy Agency (IAEA) is an independent intergovernmental organization tasked by the United Nations to monitor nuclear technology related matters. In 1979 the U.N. assigned the IAEA the task of Non-Proliferation Treaty (NPT) monitoring and for developing nuclear safeguards. In addition to monitoring activities, IAEA attempts to facilitate the safe and peaceful use of nuclear power for the generation of electricity and to assist health agencies in developing standards that protect against detrimental ionizing radiation. IAEA scientists and engineers offer specific advice regarding the safe operation of nuclear power stations and the disposal of radioactive waste.

With a staff of nearly 3000, including more than 600 field inspectors, IAEA currently serves 134 member states and maintains its headquarters in Vienna, Austria. As of May 2003, Mohamed El Baradei was serving as director-general of IAEA.

Nuclear detection technologies (many developed by the United States national laboratory system) allow IAEA inspectors to attempt to enhance security of nuclear materials and to deter the unintentional transfer of nuclear materials and nuclear technology to terrorists or nations seeking to develop nuclear weapons.

**Limitations of the IAEA.** The IAEA has no enforcement authority and compliance with IAEA inspections is voluntary; enforcement actions must be mandated by the United Nations Security Council.

Scientists also criticize the fact that IAEA leadership is composed of former civil servants or diplomats rather than scientists. Despite an expert staff of scientists, political forces have sometimes thwarted IAEA inspectors. The IAEA has suffered notable failures, including the discovery of Iraqi nuclear weapons development facilities in the early 1990s after declarations by the then IAEA chief, Hans Blix, that Iraq had no viable nuclear weapons program.

IAEA monitors selected industrial processes, namely enrichment plants, fuel-fabrication facilities, and reprocessing facilities; but military nuclear materials are not tracked by the IAEA. Accordingly, the civil inventories of the largest nuclear-power states (i.e., the United States,

United Kingdom, China, France, and Russia) are not subject to IAEA safeguards. Approximately 24 tons of weapon-grade plutonium and uranium—less than 1% of the world stock—is safeguarded by IAEA. Although a small percentage, this material is critical because it could produce hundreds of nuclear weapons. Moreover, intelligence experts consider the IAEA monitored sites to be among those sites most vulnerable to potential diversion of nuclear materials.

**IAEA actions.** Following the 1986 Chernobyl disaster in the former Soviet Union (now Ukraine) IAEA inspectors and technical teams helped stabilize the damaged reactor. IAEA continued its role at Chernobyl to include the ongoing decommissioning of the facility.

IAEA inspectors took a lead role in controversial inspections programs in Iraq, North Korea, and Iran.

In 1991, IAEA's Iraq Action Team began inspecting suspect sites in Iraq under U.N. Security Council mandate. IAEA's mandate in Iraq was two-fold: uncover and dismantle Iraq's clandestine nuclear program, and manage an ongoing monitoring and verification plan (OMV). Prior to the invasion of Iraq by U.S.-led Coalition forces in March 2003, El Baradei, reported to the U.N. that Iraq had apparently been unable to successfully reconstitute its nuclear weapons program following its destruction and dismantling in the early 1990s.

IAEA inspectors have been consistently frustrated in their attempts to deal with North Korea. In 1999, IAEA officials reported to the United Nations Security Council that "critical parts" of the North Korean reactor at Yongbyon had been unaccounted for since 1994. Missing parts included those needed to control nuclear reactions and/or those that would be needed to construct another nuclear reactor. Special requests for inspections continued to be rejected by North Korea and in April 1993, the IAEA reissued its early 1990s ruling that North Korea was in "non-compliance" with its agreements regarding nuclear inspection and safeguards. IAEA inspectors further concluded that their limited inspections could not provide "meaningful assurance" that North Korea was using its nuclear facilities for peaceful purposes (e.g., only for energy generation or authorized research).

Concerned that Iran was attempting to accelerate its nuclear programs in such a way as to facilitate nuclear weapon development, in late 2002, IAEA inspectors requested additional access to inspect Iranian facilities. IAEA requests were initially denied. In February 2003, however, IAEA inspectors, including IAEA chief inspector Mohamed El Baradei were permitted to visit several new nuclear sites in Iran.

Since 1993, the IAEA has reported more than 400 cases of trafficking in nuclear materials. While 18 cases involved plutonium or weapons-grade uranium, most cases involved low-level medical and industrial radioactive waste, the kind used in dirty bombs.

## ■ FURTHER READING :

### ELECTRONIC:

IAEA News Update on IAEA and North Korea. IAEA. <<http://www.iaea.org/worldatom/Press/Focus/iaeaDprk/>> (March 10, 2003).

International Atomic Energy Agency (IAEA). 2003. <<http://www.iaea.org/worldatom/>> (April 2, 2003).

Lu, Ming-Shih. "The IAEA Strengthened International Safeguards System." Brookhaven National Laboratory. 1998. <<http://www.nautilus.org/library/security/papers/LuSODARCO.PDF>> (April 2, 2003).

### SEE ALSO

*Iranian Nuclear Programs*  
*Iraq War: Prelude to War (The International Debate Over the Use and Effectiveness of Weapons Inspections)*  
*Los Alamos National Laboratory*  
*Nonproliferation and National Security, United States*  
*North Korean Nuclear Weapons Programs*  
*Nuclear Power Plants, Security*  
*Nuclear Regulatory Commission (NRC), United States*  
*Russian Nuclear Materials, Security Issues*  
*Weapon-Grade Plutonium and Uranium, Tracking*

---

## International Narcotics and Law Enforcement Affairs (INL), United States Bureau of

---

The Bureau for International Narcotics and Law Enforcement Affairs (INL) is an office of the U.S. State Department that advises the president, the secretary of state and other bureaus within the State Department, and other departments and agencies of the federal government on U.S. programs to combat international drug trafficking and other crimes. Its efforts support two strategic goals of the State Department: to reduce the flow of illegal drugs into the United States, and to minimize the impact of international crime within the country and among American citizens. As such, since the time of its founding in 1978, it has experienced a shift of focus from efforts against the drug trade to a larger anti-crime mission.

Recognizing the increased internationalization of drug-related crime, the State Department in 1978 created the Bureau of International Narcotics Matters (INM). Its efforts were directed toward support of police activities against the drug trade in far-flung corners of the world. Then, in November 1993, President William J. Clinton expanded its mission in Presidential Decision Directive (PDD) 14. Thereafter INM would also undertake military and economic/security assistance for drug control. The name was changed to the INL in 1995.

Today INL is known by the nickname “drugs and thugs.” The nickname was the result of a broadened mandate pursuant to PDD 14, which saw an expansion of INM’s focus in the period 1993–94. In addition to drugs, INM would thenceforth be concerned also with money laundering, international traffic in stolen vehicles, sales of arms and other contraband, smuggling of illegal aliens, and other varieties of crime at a transnational level. Accordingly, INM’s name was changed early in 1995 to reflect the breadth of its new mission.

Working with domestic drug law-enforcement and regulatory agencies, INL acts as a U.S. representative on international bodies concerned with the drug trade. It promotes those aspects of U.S. foreign relations that can be used to stop the production of illegal drugs, and their smuggling into the United States. It advises the Secretary of State and other federal bureaus on issues of international drug control, and prepares the annual *International Narcotics Control Strategy Report* on drug production, traffic, and abuse worldwide. Additionally, it manages a drug control certification process mandated in a 1986 law.

A large portion of INL’s budget, which in 1997 was \$195 million (with an additional \$20 million for criminal justice programs), is directed toward drug control assistance in some 85 countries. A great deal of these funds go to the Drug Enforcement Administration, Coast Guard, U.S. Customs Service, and other agencies that train foreign law-enforcement personnel in drug interdiction techniques. Particular attention and effort is directed toward those countries that loom large as sites for the production or transit of drugs, an array that ranges from the Bahamas to Pakistan, and from Colombia to Thailand. These and many other nations have INL narcotics affairs sections, which may consist of a single individual, or (in the case of Bolivia, Colombia, and Peru) may include dozens of foreign service officers, contractors, and Department of Defense pilots.

**Efforts against international crime.** In accordance with its expanded mission since the mid-1990s, INL has been involved in numerous efforts, not just against drugs, but against “thugs” as well. It has issued warnings against advance fee business scams, many of which originate from Nigeria and other parts of west Africa, and which typically involve a fax or e-mail requesting assistance in transferring a large amount of money. In the end, after the perpetrator has gotten hold of the target’s bank account numbers or other sensitive information, the only transfer of funds is to the perpetrator. INL, in an advisory on the subject, indicated that persons receiving such a proposition should refer it to law enforcement officials. In another advisory, INL counseled Americans traveling abroad never to get involved in drug smuggling, because the best that the U.S. consul can do for a jailed American is to ensure that he or she will be treated in accordance with local law that in many cases is far more severe and restrictive of individual rights than U.S. law.

INL does more than advise: as with drugs, it has been involved in efforts against those who smuggle in aliens from China and other countries to become virtual slaves as payment for their tickets. It also works to counter international insurance fraud, such as that involving international car-theft rings operating in the United States. Often the cars stolen are leased vehicles, and the “owner,” rather than turn in the car and pay a large fee for driving it too many miles, arranges to have it stolen, and collects the insurance money along with a fee from the car-theft ring. Such insurance fraud costs the U.S. consumer hundreds of dollars a year in increased premiums and indirect costs.

In an effort to enhance crime-fighting efforts internationally, INL in the 1990s cooperated with other U.S. law enforcement agencies to establish several International Law Enforcement Academies (ILEAs) overseas. Among the ILEAs established are facilities in Budapest, Hungary (1995); Bangkok, Thailand (1998); and Gabarone, Botswana (2001). In 2001, INL also opened an ILEA in Roswell, New Mexico.

#### ■ FURTHER READING:

##### ELECTRONIC:

Bureau for International Narcotics and Law Enforcement Affairs. <<http://www.state.gov/g/inl/>> (March 19, 2003).

##### SEE ALSO

*DEA (Drug Enforcement Administration)*  
*Department of State, United States*  
*Drug Control Policy, United States Office of National*  
*Interpol (International Criminal Police Organization)*  
*Law Enforcement, Responses to Terrorism*  
*NDIC (Department of Justice National Drug Intelligence*  
*Center)*

---

## Internet

---

#### ■ JUDSON KNIGHT

The Internet is a vast worldwide conglomeration of linked computer networks. Its roots lie in the mid-twentieth century, with a number of projects by the United States government and the private sector, most notable of which was the computer network created by the Advanced Research Projects Agency (ARPA) of the Department of Defense (DOD) in 1969. Until the early 1990s, the Internet remained largely the province of specialists, including defense personnel and scientists. The creation of browsers, or software that provided a convenient graphical interface between user and machine, revolutionized the medium, and spawned rapid economic growth throughout the 1990s. In addition to the World Wide Web and e-mail, the parts of the Internet most familiar to casual users, the Internet



A U.S. college student is arrested by FBI agents in Los Angeles, California, for the perpetration of an Internet hoax in 2000, in which he made over \$241,000 and lost a Southern California high-tech company billions of dollars in market value. ©AFP/CORBIS.

contains a frontier that offers both great promise and great challenges to law and security.

## Birth of the Internet

The basis of the Internet is the network, a group of computers linked by communication lines. The distant ancestors of today's networks were highly specialized systems used either by DOD, or by private companies (for example, airlines, which tracked reservations on the SABRE system) during the late 1950s and early 1960s. The development of semiconductor technology in the 1960s enabled the growth of computer activity in general, and networking in particular. Universities and research centers participated in time-sharing, whereby multiple users accessed the same system.

ARPANET, which connected time-sharing facilities at research centers, is generally regarded as the first true computer network. It provided a testing-ground for technologies that are still used today: simple mail transfer protocol (SMTP), the system that makes e-mail possible, and file transfer protocol (FTP), for transmitting large messages. To maximize effectiveness, ARPANET broke messages into small pieces, or packets, that could easily be transmitted and reassembled. The technique, known as

packet switching, enhanced communication between computers.

**The 1970s: TCP/IP.** During the 1970s, ARPA (now known as the Defense Advanced Research Projects Agency, or DARPA) continued its efforts to connect its users, but it eventually ran into a dead-end posed by the primitive systems of networking used at the time. Faced with this roadblock, DARPA turned to two computer scientists, Vinton Cerf and Robert Kahn, who developed a design that revolutionized networks.

This was the transmission control protocol (TCP), which, coupled with the related Internet Protocol (IP), provided a mechanism for addressing messages and routing them to their destinations using an open architecture that connected standardized networks. In 1980, DOD adopted TCP/IP as its standard, and required all participants to adopt the protocol as of January 1, 1983. Some observers regard this event as the true birth of the Internet.

**The 1980s: civilian agencies get involved.** The 1980s saw use of computer networks expand to include civilian agencies. Among these was the National Science Foundation (NSF),

which worked with five supercomputing centers spread across the country to create NSFNET, a “backbone” system intended to connect the entire nation. NSF succeeded in linking small local and regional networks to NSFNET. Other civilian participants in computer networks, which began to increasingly overlap with one another, included the Department of Energy and the National Aeronautics and Space Administration (NASA), as well as a number of private companies.

Also during this period, several independent consortiums took on themselves the task of organizing and policing the rapidly growing Internet. Among these were the Internet Engineering Task Force and the Internet Society, both of which are concerned with Internet standards, as well as the Internet Corporation for Assigned Names and Numbers (ICANN). The latter controls policy with regard to the assignment of domain names, including top-level domains such as *.com* for commercial enterprises, *.gov* for government offices, *.edu* for schools, and so on.

## The Internet Explosion

The mid-1980s saw the birth of the first commercial computer networks, including Prodigy, CompuServe, and Quantum Computer Services. The first two would eventually recede in significance as larger companies took over the Internet, but the third—founded in 1985 and renamed America Online (AOL) in 1989—would eventually merge with publishing and entertainment conglomerate Time Warner to control a wide span of media. All of that lay far in the future, however, during the mid-1980s, as the few commercial participants developed their first subscriber bases and linked up to NSFNET through the Commercial Internet Exchange (CIX).

A number of technological innovations in the 1980s and early 1990s portended the explosive growth of the Internet that would take place in the next decade. Among these was the development of the personal computer or PC, as well as local area networks (LANs), which linked computers within a single business or location. NSFNET, working with the Corporation for National Research Initiatives, sponsored the first commercial use of e-mail on the Internet. Then, in 1993, new legislation at the federal level permitted the full opening of the NSFNET to commercial users.

The result was much like the opening of lands in the western United States to homesteaders, only the “land” in this case existed in virtual or cyberspace, and instead of wagons, the new settlers used browsers. The first important browser was Mosaic, developed at the University of Illinois using standards created at the European Organization for Nuclear Research (CERN) by Tim Berners-Lee. Thus was born the World Wide Web, which uses hypertext transfer protocol, or HTTP. In this environment, Mosaic—known as Netscape Navigator after the formation of the Netscape Communications Corporation in 1994—and Microsoft’s competing Internet Explorer would prove the most useful navigating tools.

Users of the Internet today can still travel to regions beyond the World Wide Web, where they can see what the Internet was like prior to 1993. The most significant surviving portion of this older section is Usenet, a worldwide bulletin board system containing some 14,000 forums or newsgroups. In addition to the Web and Usenet, the Internet includes e-mail (electronic mail), FTP sites (used for transferring pictures and other large files), instant messaging, and other components. At the edges of the Internet are proprietary services such as those accessible only to AOL users, as well as other pay sites. Additionally, company and government intranets (private networks accessible only through a password) lie beyond the periphery of the Internet, though a browser may be used to access both.

By 1988, the size of the Internet was doubling every year, and the advent of browsers made possible an enormous consumer influx. The mid- to late 1990s saw the formation of thousands of Internet service providers (ISPs), through which users gained access to the Internet in exchange for a monthly fee. As competition increased, fees decreased, forcing consolidation of providers. By the beginning of the twenty-first century, major companies such as AOL, AT&T, and Earthlink, along with a few second-tier ISPs, controlled most of the market.

The explosive growth of the Internet itself, coupled with the expanded opportunities for commerce it provided, fueled one of the greatest periods of economic growth in U.S. history, from 1996 to 2000. The economic downturn that began in April, 2000, and continued throughout the early 2000s, however, served as an indicator that the Internet—while it had certainly transformed communications—would not solve all problems.

There were several problems associated with the Internet itself, and simplest among these were the technological challenges involved in moving ever larger amounts of data. By the beginning of the twenty-first century, it became possible to access video and complex graphics using powerful data streams, and computer scientists envisioned technology that would make possible the use of high-resolution video or multiple streams on networks capable of processing 100 gigabits of data a second. To expand the number of available addresses, hitherto limited by the 32-bit IP address standard, the Internet Engineering Task Force in 1998 approved a new 128-bit standard. This made possible so many addresses that every electronic device in the world could have its own unique location in an ever-expanding Internet.

Less simple were some of the challenges associated with human activities. There were cybercrimes, such as hacking or the dissemination of viruses, either of which could be used simply as a form of information-age vandalism, or for extortion. Hacking of financial service sites also offered the opportunity to commit robbery without picking locks, and for this reason many companies adopted secure, encrypted sites. (The latter were designated by the prefix *https://*, in contrast to the ordinary *http://*.)



Just as the Internet could be used for education, commerce, and a host of other purposes, it also provided a forum for activities that tested the limits of free speech; extremist political parties and hate groups could operate a Web site. On the other hand, use of the Web to distribute drugs, weapons, or child pornography carried stiff penalties. At the same time, government attempts to restrict or control aspects of the Internet raised concerns over the abrogation of First Amendment rights. The Internet itself was worldwide, beyond the reach of even the U.S. Constitution or any law, and although China's totalitarian regime attempted to restrict citizens' access to it, the network continued to work its way deeper and deeper into the fabric of modern life.

#### ■ FURTHER READING:

##### BOOKS:

- Gillies, James, and R. Cailliau. *How the Web Was Born: The Story of the World Wide Web*. New York: Oxford University Press, 2000.
- Hafner, Katie, and Matthew Lyon. *Where Wizards Stay Up Late: The Origins of the Internet*. New York: Simon & Schuster, 1996.
- Young, Gray, ed. *The Internet*. New York: H. W. Wilson, 1998.

##### ELECTRONIC:

- Defense Advanced Research Projects Agency. <<http://www.darpa.mil/>> (April 14, 2003).
- Internet Society. <<http://www.isoc.org/>> (April 14, 2003).
- Webopedia: Online Dictionary for Computer and Internet Terms. <<http://www.webopedia.com/>> (April 14, 2003).

##### SEE ALSO

**CERN**  
*Computer Hackers*  
*Computer Software Security*  
*Computer Virus*  
*DARPA (Defense Advanced Research Projects Agency)*  
*Internet: Dynamic and Static Addresses*  
*Internet Spam and Fraud*  
*Internet Spider*  
*Internet Surveillance*  
*Internet Tracking and Tracing*  
*NSF (National Science Foundation)*

---

## Internet: Dynamic and Static Addresses

---

Every computer operating on the Internet has a unique IP, or Internet protocol, address. Because the Internet's original design did not take into account the vast size it would assume from the mid-1990s onward, as more and more people went online, the architecture did not account for an

infinite number of IP addresses. To conserve these, an Internet service provider (ISP) has a limited number of permanent IP addresses, and issues temporary IP addresses for customers to use while online. The permanent and temporary IP locations are known as static and dynamic addresses, respectively.

An IP address takes the form of a dot address, or a dotted quad, that looks something like this: 123.456.789.000. Each of the three-digit numbers represents 8 bits of information, forming a 32-bit address that defines the Internet protocol. Because the Internet is really a network connecting various smaller computer networks, the IP address begins with data indicating the particular network to which a computer belongs. For very large networks, a great portion of the IP number gives the local address, whereas for extremely small networks, the majority of the address identifies the network, with only the last few numbers serving as a unique identifier.

In cases of computer crime or espionage, an IP address—sometimes described as a “social security number”—can be used to pinpoint the computer used. Naturally, a dynamic address is more desirable for concealment, just as a person who does not want a telephone call traced to his or her home may place the call from a payphone. Even so, the dynamic IP address can usually be traced to a network. In any case, dynamic addresses are likely to disappear from the scene, due to the adoption of a 128-bit Internet protocol, IPv6. Together with allocation technology known as supernetting or CIDR (Classless Inter-Domain Routing), IPv6 will make it possible to assign every computer a static IP address.

#### ■ FURTHER READING:

##### BOOKS:

- Gelman, Robert B., and Stanton McCandlish. *Protecting Yourself Online: The Definitive Resource on Safety, Freedom, and Privacy in Cyberspace*. New York: HarperEdge, 1998.
- Schneider, Bruce. *Secrets and Lies: Digital Security in a Networked World*. New York: John Wiley, 2000.
- Schwartz, Winn. *Cybershock: Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorists, and Weapons of Mass Disruption*. New York: Thunder's Mouth Press, 2000.

##### PERIODICALS:

- Cholewka, Kathleen. “Address Management Made Easier?” *Telephony* 234, no. 1 (January 5, 1998): 39.
- Ng Ken Boon. “Enabling Net Connection Sharing.” *InternetWeek* no. 872 (August 6, 2001): 1.
- Prince, Paul. “Static Electricity.” *Tele.com* 6, no. 17 (September 3, 2001): 28.

##### SEE ALSO

*Computer Hackers*  
*Cyber Security*  
*Internet Spam and Fraud*  
*Internet Spider*

*Internet Surveillance*  
*Internet Tracking and Tracing*

---

## Internet Spam and Fraud

---

■ K. LEE LERNER

An increasingly costly and vexing economic security issue involves the high traffic in unsolicited commercial email (termed "spam") and the use of internet communication to commit fraud.

Nearly one-half of the estimated 50 billion email messages sent each day are spam mail that contain usually misleading or fraudulent representations for products or services ranging from health and well-being products to pornography. Internet experts assert that nearly 90 percent of the spam mail sent is sent by a network of less than 200 individuals or direct marketing companies that use spam. Spam is costly to Internet service providers (ISP) and to consumers in terms of money, time, and bandwidth. Spam can also disrupt the normal operation of many network systems. Current efforts to curb spam involve legal restrictions and technical measures to block the transfer of such messages.

Spam technology commonly exploits openings in the program structure of computers (e.g. open proxies, etc.) attached to the Internet that are then designated to act as relays for sending spam. Spammers use special programs to identify vulnerable computers. Messages relayed from these computers often carry only the "innocent" relaying computer's identification. Special internet spiders can also be used by spammers to extract email addresses from websites.

In late April 2003, the state of Virginia enacted tough anti-spam laws and congressional leaders promised action on similar measures at the federal level. One legislative initiative, the "Can Spam Act," would include civil fines for senders of commercial e-mail with fraudulent or otherwise invalid return email addresses. Virginia's law potentially subjects repeat or "serial" spammers to felony penalties. That tough legislation was first passed in Virginia is significant because Virginia hosts a number of major Internet hubs and providers, including the United States' largest ISP, America Online.

The first anti-spam bill was passed by Nevada in 1997, and about half of all states have such laws. Some simply require that bulk email senders offer email recipients a method to prevent further mailings from a particular sender. Other laws prohibit false identifiers, misleading subject headings or require unsolicited e-mail to be identified with "ADV" in the subject line. Messages with a characteristic label or portion of text in their subject line are more easily filtered from email traffic. Conventional filters can also scan email for characteristic strings of text such as "no

prescription required" that often accompany fraudulent email related to drugs normally available only by prescription. Other Congressional proposals include the potential creation of a national registry of addresses who do not want to receive spam.

Within the United States, the Federal Trade Commission (FTC) is responsible for internet commercial regulation and has acted to stop spamming by use of anti-fraud laws.

### ■ FURTHER READING:

#### BOOKS:

Mulligan, Geoff. *Removing the Spam: Email Processing and Filtering*. Boston: Addison-Wesley Publishing, 1999.

#### PERIODICALS:

Frank, Diane. "Cybersecurity Center Takes Shape." *Federal Computer Week* 16, no. 4 (February 18, 2002): 10.

#### SEE ALSO

*Computer and Electronic Data, Destruction*  
*Computer Fraud and Abuse Act of 1986*  
*Computer Hackers*  
*Computer Keystroke Recorder*  
*Computer Software Security*  
*Computer Virus*  
*Internet: Dynamic and Static Addresses*  
*Internet Spider*  
*Internet Surveillance*  
*Internet Tracking and Tracing*

---

## Internet Spider

---

An Internet spider is a program designed to "crawl" over the World Wide Web, the portion of the Internet most familiar to general users, and retrieve locations of Web pages. It is sometimes referred to as a webcrawler. Many search engines use webcrawlers to obtain links, which are filed away in an index. When a user asks for information on a particular subject, the search engine pulls up pages retrieved by the Internet spider. Without spiders, the vast richness of the Web would be all but inaccessible to most users, rather as the Library of Congress would be if the books were not organized.

Some search engines are human-based, meaning that they rely on humans to submit links and other information, which the search engine categorizes, catalogues, and indexes. Most search engines today use a combination of human and crawler input. Crawler-based engines send out spiders, which are actually computer programs that have sometimes been likened to viruses because of their ability to move between, and insert themselves into, other areas in cyberspace.

Spiders visit Web sites, record the information there, read the meta tags that identify a site according to subjects, and follow the site's links to other pages. Because of the many links between pages, a spider can start at almost any point on the Web and keep moving. Eventually it returns the data gathered on its journey to the search engine's central depository of information, where it is organized and stored. Periodically the crawler will revisit the sites to check for changed information, but until it does so, the material in the search engine's index remains the same. It is for this reason that a search at any time may yield "dead" Web pages, or ones that can no longer be found.

No two search engines are exactly the same, the reason being (among other things) a difference in the choice of algorithm by which the indices are searched. Algorithms can be adjusted to scan for the frequency of certain keywords, and even to circumvent attempts at keyword stuffing or "spamdexing," the insertion of irrelevant search terms intended simply to draw traffic to a site.

#### ■ FURTHER READING :

##### BOOKS:

Fah-Chun Cheong. *Internet Agents: Spiders, Wanderers, Brokers, and 'Bots*. Indianapolis, IN: New Riders, 1996.

Sherman, Chris, and Gary Price. *The Invisible Web: Uncovering Information Sources Search Engines Can't See*. Medford, NJ: CyberAge Books, 2001.

Young, Gray. *The Internet*. New York: H. W. Wilson, 1998.

##### SEE ALSO

*Computer Virus*

*Internet: Dynamic and Static Addresses*

*Internet Spam and Fraud*

*Internet Surveillance*

*Internet Tracking and Tracing*

---

## Internet Surveillance

---

#### ■ LARRY GILMAN

Internet surveillance is the monitoring of Internet data traffic for information useful to government authorities.

Targeted content may be illegal (e.g., child pornography), politically suspect (e.g., human-rights websites accessed by citizens living under authoritarian regimes), or evidential (e.g., e-mails or voice messages exchanged by suspects). Because the volume of information passing through the Internet is large, Internet surveillance generally requires a software component that scans for selected patterns of text, speech, addressing, or usage, and which flags items of interest for inspection by a human operator. Countermeasures against Internet surveillance include

avoidance of the Internet as a means of communication, the establishment of Internet aliases that conceal users' identities, and encryption.

**Levels of Internet surveillance.** Internet surveillance may target individuals, local networks, or Internet traffic in bulk. Surveillance of individual users (or, rather, of individual electronic addresses, which may actually have more than one user) is analogous to traditional telephone wiretapping: a law-enforcement agency, intelligence agency, or other surveillant first gains physical access to one or more computers through which the Internet traffic of a suspect party passes. Using specialized hardware and software, the surveillant then scans all data traffic passing to and from the targeted party. Some or all of that traffic may be recorded by the surveillant for later use. All transmissions, recorded or not, are allowed to continue on to their intended destinations so that the surveillance remains secret.

Surveillance systems have been proposed recently that would scan Internet content and usage patterns in bulk, not user-by-user. For example, in December 2002 the President's Critical Infrastructure Protection Board released a report entitled "The National Strategy to Secure Cyberspace" (<http://www.whitehouse.gov/pcipb/>). This report urged the creation of a centralized computer system to monitor the Internet. Such monitoring might, the paper said, be restricted to the analysis of network usage patterns (e.g., a wave of e-mails possibly indicating the spread of a new computer virus via the Internet), rather than being empowered to examine message content. Non-content information that might be gleaned by such a surveillance system includes the source and destination addresses of e-mails, the electronic addresses of websites visited by various persons, or the electronic addresses of persons visiting various websites. However, it would probably be impractical to build a high-level monitoring system that did not provide, at least potentially, access to individual users' information.

**Uses and abuses.** Many governments are interested in Internet surveillance, whether to fight crime and terrorism, monitor the political speech of their citizens, or both. For example, immediately after the terrorist attacks of September 11, 2001, the British government asked British Internet service providers (ISPs) to temporarily record all their users' Internet traffic, hoping that clues to the attacks might be preserved. Various authoritarian governments block access to certain websites or spy on users to enforce political conformity, including the governments of Laos, Myanmar, Saudi Arabia, Syria, the United Arab Emirates, and Yemen. China monitors public Internet use for political keywords such as "June 4" (the date of the 1989 pro-democracy protests in Tiananmen Square, which the Chinese government violently suppressed), and maintains "public security bureaus" around the country to monitor Internet traffic. As of February 2003, China has jailed at

least 33 people for forbidden Internet use of a political nature, including downloading of articles from foreign pro-democracy websites. In the U.S. and many other countries it is illegal for the government to spy on citizens' nonviolent political activities, whether via Internet surveillance or by other means; however, there is evidence that these laws have been tested in the past and, some experts argue, might be broken even more readily using powerful, impossible-to-detect Internet surveillance tools such as are already in use or technically feasible. The topic of Internet surveillance is thus fraught with political controversy.

In 2002, for example, the U.S. Defense Advanced Research Projects Agency (DARPA)—the same branch of the Pentagon that created the beginnings of the Internet—proposed an ambitious Internet surveillance system termed Total Information Awareness (TIA). TIA would, according to DARPA, not only allow access to the content of virtually the whole Internet, but would enable the government to integrate that information with data gained by virtually any other means: wiretaps, criminal and other public records, on-line shopping habits, credit-card use, automated tollbooth data, cell-phone calling records, and so on. TIA bids for information omniscience.

However, the TIA proposal met instant protest from across the political spectrum, and in January 2003 the U.S. Senate voted restrictions on its development and deployment. Development of TIA cannot, the Senate has said, continue unless the president certifies that halting it “would endanger the national security of the United States.” (As of this writing, the president has not yet made any such certification.) The political future of TIA is therefore doubtful; there is, however, little doubt about its technical feasibility.

In a similar vein, the U.S. National Security Agency (NSA), whose official mission is eavesdropping on communications outside the U.S. and across its borders and which has a bigger budget than the Central Intelligence Agency, is thought by some analysts to already have a system (“Echelon”) that can scan Internet message traffic for nonencrypted keywords. Since other governments certainly possess such software, there cannot be any technical obstacles to its development by the NSA; however, as of February 2003 the existence of Echelon remains unconfirmed.

In the meantime, the U.S. Federal Bureau of Investigation (FBI) routinely employs the Carnivore program for Internet surveillance of individuals. Carnivore, whose use has been publicly acknowledged by the FBI since June 2000, is classified as a “high-speed packet sniffer” (a term explained below). It is part of a larger surveillance toolbox called the Dragonware Suite. Dragonware is comprised of three software tools: Carnivore, Packeteer, and Coolminer. No public information about Packeteer and Coolminer is available, but some experts assert that these programs organize the information collected by Carnivore and analyze it for various patterns (probably under the guidance of human users).

**What “Carnivore” does.** Binary information streaming over the Internet is organized into “packets.” Each packet is a collection of bits containing both message content and information about where it has come from and where it is going to. Data to be transmitted over the Internet are thus not sent as a continuous stream of 1s and 0s over dedicated channels, but as a blizzard of tiny, independent messages (packets) that may follow different paths to their final destination. They are reassembled at the receiving party’s ISP before final transmission to the user over a dedicated line (e.g., a telephone line). A packet sniffer examines (“sniffs”) every packet being handled by an ISP to see if its source or destination are on a target list of electronic addresses. The packet sniffer may be set either to simply record all packets meeting these criteria or to further examine each packet to see if its content matches court-mandated search guidelines (e.g., mention of bombs, drugs, insider trading). If a packet’s content does not match search-order guidelines, it is not recorded. Alternatively, the packet sniffer may ignore content altogether, recording only routing information (source and destination addresses).

Use of Carnivore is governed by the Electronic Communications Privacy Act of 1994 (ECPA) and by the federal law governing wiretaps, the Wire and Electronic Communications Interception and Interception of Oral Communications Act (also known as Title III). These laws state that officials need to obtain a search warrant from a court in order to look at stored digital data such as e-mails held in memory by an ISP or the contents of a user’s hard drive. They also state that a court order must be obtained before a program such as Carnivore can be used to monitor communications in real time (e-mails in transit, for example). There are several kinds of court orders authorizing Internet surveillance, each allowing different information to be collected: (1) a *content wiretap* allows the recording of all information in packets that meet certain criteria (e.g., mention of a specific activity or person); (2) a *trap-and-trace* wiretap allows the FBI only to record information about destinations and websites visited, not content; (3) a *pen register* wiretap, like a trap-and-trace in reverse, determines where e-mail received by the suspect party has come from, what the electronic addresses are of parties that access the suspect’s website, and so forth. Again, a pen register wiretap is not authorized to record content.

**Controversy.** Like almost any technical tool, Internet surveillance can be used for both legitimate and illegitimate purposes. Unfortunately, all official organizations, in all countries, declare that they are legitimate and that the individuals they surveil are dangerous criminals. In the U.S., the FBI and DARPA defend Internet surveillance tools like Carnivore and TIA by pointing out that they are only supposed to be used as authorized by a federal court (in the case of Carnivore) or to preserve national security (in the case of the proposed TIA program). According to the FBI, “The ability of law enforcement agencies to conduct lawful electronic surveillance of the communications of its

criminal subjects represents one of the most important capabilities for acquiring evidence to prevent serious criminal behavior." John Poindexter, head of the Information Awareness Office (part of DARPA), which is developing TIA, says that the U.S. needs TIA because "[w]e must be able to detect, classify, identify, and track terrorists so that we may understand their plans and act to prevent them from being executed."

Critics such as the American Civil Liberties Union argue that what the FBI and the intelligence agencies are supposed to do is not always the same as what they have done; there is a long public record of potentially illegal political surveillance of U.S. citizens by U.S. police and government organizations. Therefore, critics argue, certain tools—especially those that would make it possible to filter the Internet transactions of thousands or millions of people simultaneously—should not even be developed, whereas those with lesser capabilities, such as Carnivore, should operate under more severe restrictions than they presently do.

#### ■ FURTHER READING:

##### PERIODICALS:

Lee, Jennifer. "Guerilla Warfare, Waged with Code." *New York Times*. October 10, 2002.

Markoff, John, and John Schwartz. "Bush Administration to Propose System for Monitoring Internet." *New York Times*. December 20, 2002.

McCullagh, Declan. "FBI Agents Soon May Be Able to Spy on Internet Users Legally Without a Court Order." *New York Times*. September 14, 2001.

##### ELECTRONIC:

Poindexter, John. "Overview of the Information Awareness Office." Defense Advanced Research Projects Agency. August 2, 2002. <<http://www.fas.org/irp/agency/dod/poindexter.html>> (Jan. 28, 2003).

##### SEE ALSO

*Cyber Security*

## Internet Tracking and Tracing

■ BRIAN HOYLE

Electronic passage through the Internet leaves a trail that can be traced. Tracing is a process that follows the Internet activity backwards, from the recipient to the user. As well, a user's Internet activity on web sites can also be tracked on the recipient site (i.e., what sites are visited and how often). Sometimes this tracking and tracing ability is used to generate email to the user promoting a product that is related to the sites visited. User information, however, can also be gathered covertly.

Techniques of Internet tracking and tracing can also enable authorities to pursue and identify those responsible for malicious Internet activity. For example, on February 8, 2000, a number of key commercial Internet sites such as Yahoo, Ebay, and Amazon were jammed with incoming information and rendered inoperable. Through tracing and tracking techniques, law enforcement authorities established that the attacks had arisen from the computer of a 15-year-old boy in Montreal, Canada. The youth, whose Internet identity was "Mafiaboy," was arrested within months of the incidents.

Law enforcement use of Internet tracking is extensive. For example, the U.S. Federal Bureau of Investigation has a tracking program designated Carnivore. The program is capable of scanning thousands of emails to identify those that meet the search criteria.

### Tracking Tools

**Cookies.** Cookies are computer files that are stored on a user's computer during a visit to a web site. When the user electronically enters the web site, the host computer automatically loads the file(s) to the user's computer.

The cookie is a tracking device, which records the electronic movements made by the user at the site, as well as identifiers such as a username and password. Commercial web sites make use of cookies to allow a user to establish an account on the first visit to the site and so to avoid having to enter account information (i.e., address, credit card number, financial activity) on subsequent visits. User information can also be collected unbeknownst to the user and subsequently used for whatever purpose the host intends.

Cookies are files, and so can be transferred from the host computer to another computer. This can occur legally (i.e., selling of a subscriber mailing list) or illegally (i.e., "hacking in" to a host computer and copying the file). Also, cookies can be acquired as part of a law enforcement investigation.

Stealing a cookie requires knowledge of the file name. Unfortunately, this information is not difficult to obtain. A survey, conducted by a U.S. Internet security company in 2002, on 109, 212 web sites that used cookies found that almost 55 percent of them used the same cookie name. Cookies may be disabled by the user, however, this calls for programming knowledge that many users do not have or do not wish to acquire.

**Bugs or Beacons.** A bug or a beacon is an image that can be installed on a web page or in an email. Unlike cookies, bugs cannot be disabled. They can be prominent or surreptitious. As examples of the latter, graphics that are transparent to the user can be present, as can graphics that are only 1x1 pixels in size (corresponding to a dot on a computer monitor). When a user clicks onto the graphic in an attempt to view, or even to close the image, information is relayed to the host computer.

Information that can be gathered by bugs or beacons includes:

- the user's IP address (the Internet address of the computer)
- the email address of the user
- the user computer's operating system (which can be used to target viruses to specific operating systems)
- the URL (Uniform Record Locator), or address, of the web page that the user was visiting when the bug or beacon was activated
- the browser that was used (i.e., Netscape, Explorer)

When used as a marketing tool or means for an entrepreneur to acquire information about the consumer, bugs or beacons can be merely an annoyance. However, the acquisition of IP addresses and other user information can be used maliciously. For example, information on active email addresses can be used to send "spam" email or virus-laden email to the user. And, like cookies, the information provided by the bug or beacon can be useful to law enforcement officers who are tracking down the source of an Internet intrusion.

**Active X, JavaScript.** These computer-scripting languages are automatically activated when a site is visited. The mini-programs can operate within the larger program, so as to create the "pop-up" advertiser windows that appear with increasing frequency on web sites. When the pop-up graphic is visited, user information such as described in the above sections can be gathered.

**Tracing email.** Email transmissions have several features that make it possible to trace their passage from the sender to the recipient computers. For example, every email contains a section of information that is dubbed the header. Information concerning the origin time, date, and location of the message is present, as is the Internet address (IP) of the sender's computer.

If an alias has been used to send the message, the IP number can be used to trace the true origin of the transmission. When the message source is a personally owned computer, this tracing can often lead directly to the sender. However, if the sending computer serves a large community—such as a university, and through which malicious transmissions are often routed—then identifying the sender can remain daunting.

Depending on the email program in use, even a communal facility can have information concerning the account of the sender.

The information in the header also details the route that the message took from the sending computer to the recipient computer. This can be useful in unearthing the identity of the sender. For example, in the case of Mafiaboy, examination of the transmissions led to a computer at the University of California at Santa Barbara that had been commandeered for the prank. Examination of the log files

allowed authorities to trace the transmission path back to the sender's personal computer.

**Chat rooms.** Chat rooms are electronic forums where users can visit and exchange views and opinions about a variety of issues. By piecing together the electronic transcripts of the chat room conversations, enforcement officers can track down the source of malicious activity.

Returning to the example of Mafiaboy, enforcement officers were able to find transmissions at certain chat rooms where the upcoming malicious activity was described. The source of the transmissions was determined to be the youth's personal computer. Matching the times of the chat room transmissions to the malicious events provided strong evidence of the youth's involvement.

**Tracking, tracing, and privacy.** While Internet tracking serves a useful purpose in law enforcement, its commercial use is increasingly being examined from the standpoint of personal privacy. The 1984 Cable Act in the United States permits the collection of such information if the information is deemed to aid future commercial developments. User consent is required, however, if the information that is capable of being collected can exceed that needed for commerce.

#### ■ FURTHER READING:

##### BOOKS:

Bosworth, Seymour, and Michel E. Kabay, eds. *Computer Security Handbook*. New York: John Wiley & Sons, 2002.

National Research Council, Computer Science and Telecommunications Board. *Cyber Security Today and Tomorrow: Pay Now or Pay Later*. Washington, DC: The National Academies Press, 2002.

Northcutt, Stephen, Lenny Zeltser, Scott Winters, et al. *Inside Network Perimeter Security: The Definitive Guide to Firewalls, Virtual Private Networks (VPNs), Routers, and Intrusion Detection Systems*. Indianapolis: New Riders Publishing, 2002.

##### SEE ALSO

*Computer Hackers*  
*Computer Keystroke Recorder*  
*Information Security*

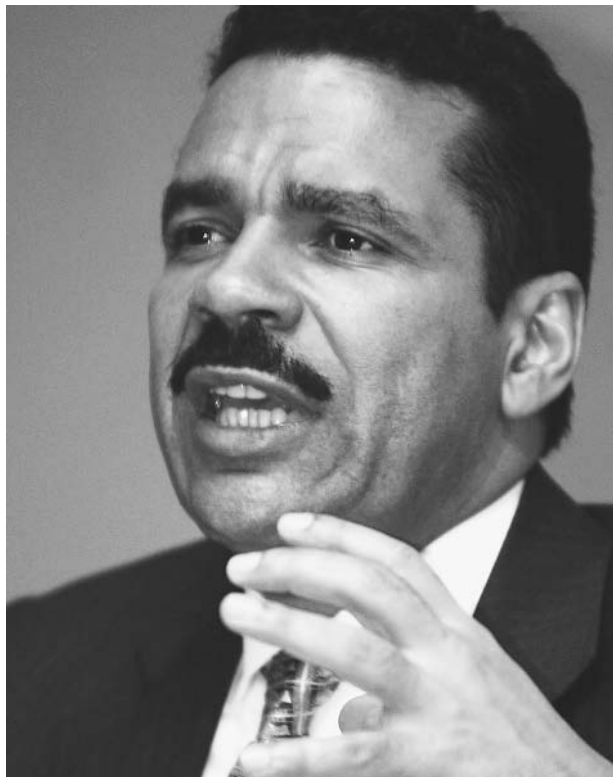
---

## Interpol (International Criminal Police Organization)

---

#### ■ CARYN E. NEUMANN

Interpol is an international organization based in Lyon, France, that fosters global police cooperation by sharing



Ronald Noble, secretary of the International Police Agency, Interpol, at a press conference in 2002, when the agency hoped to recruit three Asian countries—Afghanistan, Yajikistan, and Turkmenistan—as members to help fight international crimes and apprehend fugitives. Soon afterward, Afghanistan joined the Interpol ranks. AP/WIDE WORLD PHOTOS.

intelligence about cross-border criminal activities among its 181 member nations. Despite popular misconception, the organization maintains no police force of its own. Each member nation maintains and staffs a National Central Bureau to direct Interpol intelligence, while local authorities investigate and prosecute criminals according to national laws. Interpol's actions are limited to receiving requests for assistance; analyzing criminal activities that are not of a political, military, religious, or racial character; and disseminating notices published in four languages (English, French, Spanish, and Arabic) to its members. It currently focuses upon public safety and terrorism, organized crime, illegal drug production and smuggling, weapons dealing, trafficking in human beings, money laundering, and financial and high technology wrongdoing.

Begun in 1923, Interpol is an international effort to halt crime that has occurred or is projected to occur in multiple countries. Although headquartered in France, no country dominates the group and its funding is provided by a sliding scale membership fee that is based upon each country's gross national product (GNP). The organization's policies are set by a vote of its member countries while the governors on its executive committee are required to be drawn from different continents. The secretary general, elected every five years by two-thirds of the

members attending the annual General Assembly, is Interpol's chief executive and senior full-time official. Daily activities are conducted at the General Secretariat in Lyon with a staff of 384 who represent 54 different countries. National Central Bureaus (NCB) in member countries ferry Interpol information to appropriate local authorities who bear responsibility for apprehending and extraditing suspected criminals. Five NCBs also act as Regional Stations with Lyon covering Europe, North America, and the Middle East; Nairobi, Kenya, responsible for East Africa; Abidjan, Ivory Coast, focusing on West Africa; Buenos Aires, Argentina, addressing South America; Tokyo, Japan, transmitting to Asia; and Puerto Rico, assisting the Caribbean and Central America.

No nation is required to respond to an Interpol request. Some countries, notably the United States in the years leading up to World War II, have declined to fully cooperate with Interpol for fear that its files may be misused for the prosecution of political criminals. In 1956, the organization agreed to forbid any activities of a political, military, religious, or racial character, but concerns remain that some countries may potentially ignore these guidelines. The chief fear of many member countries is that classified information may fall into the hands of terrorists since the distribution of intelligence cannot be restricted once it enters the Interpol system. Although this worry has reduced the amount of classified information flowing through Interpol, the organization has experienced a steady increase in information traffic. In 2000, Interpol transmitted 2.5 million messages, placed 15,116 notices of criminal activity in circulation, and projected that 1400 people would be arrested or located as the result of Interpol intelligence. Interpol notices are coded into ten different colors that represent different purposes. The red wanted notices are the most common and this type of communication requests the arrest of subjects for whom an arrest warrant has been issued and extradition will be sought. The other notices are: seeking the identity and location of subjects who have committed or witnessed criminal offenses (blue); providing warning about career criminals who have committed offenses in several countries (green); seeking missing or lost people, especially children abducted by parents (yellow); seeking the identification of corpses (black); warning of unusual modus operandi (purple); sharing knowledge of organized crime groups (gray); and advising of criminal activity with international ramifications that does not involve a specific person or group (orange). Stolen property notices are also distributed but are not coded.

As the second largest international organization behind the United Nations, Interpol has a record of proven success. It continues to grow as new nations join and the organization betters its communications system. The increasing global movement of people and the concomitant jump in international crime likely means that Interpol will remain a popular crime-fighting tool well into the twenty-first century.

## ■ FURTHER READING :

### BOOKS:

Anderson, Malcolm. *Policing the World: Interpol and the Politics of International Police Co-operation*. Oxford: Clarendon Press, 1989.

Bresler, Fenton. *Interpol*. London: Sinclair-Stevenson, 1992.

United States Department of Justice and United States Department of the Treasury. *Interpol: The International Criminal Police Organization*. Washington, D.C.: Government Printing Office, 2002.

### ELECTRONIC:

Interpol. "Interpol Information." <<http://www.interpol.int/Public/lcpo/default.asp>> (January 17, 2003).

### SEE ALSO

*Classified Information*  
*Interpol (International Criminal Police Organization)*

---

## Interpol, United States National Central Bureau

---

■ CARYN E. NEUMANN

As the United States branch of Interpol, an international police organization, the National Central Bureau (NCB) in Washington, D.C., serves as a communications clearinghouse for police seeking assistance in criminal investigations that cross international boundaries. Directed by the U.S. Attorney General and representing sixteen law enforcement agencies under the Department of Justice in conjunction with the Department of the Treasury, the USNCB focuses on fugitives, financial fraud, drug violations, terrorism, and violent crimes. It can refuse to respond to any of the 200,000 annual inquiries from other nations and, as required by Interpol bylaws, does not assist in the capture of people sought for political, racial, or ethnic reasons.

Although Interpol dates back to 1923, the USNCB did not come into existence until the 1960s because of a lukewarm American attitude toward the organization. Hesitant about the benefits of international policework, the Federal Bureau of Investigation (FBI) in the Department of Justice did not post wanted notices with Interpol until 1936. When J. Edgar Hoover (1895–1972), head of the FBI from 1924 to 1972, observed Interpol's success in apprehending criminals, his subsequent support of the police force prompted Congress to order the Attorney General to

accept Interpol membership in 1938. Hoover became the permanent American representative to Interpol with only the FBI authorized to do business with the group. In 1950, Hoover pulled the FBI out of Interpol for reasons that remain unclear. The Treasury, however, continued to maintain informal contact with the organization and became the official U.S. representative in 1958. When the U.S. decided to establish an NCB in 1962 as part of Attorney General Robert F. Kennedy's fight against organized crime, the history of American involvement dictated a sharing of power between the two agencies, with Justice as the dominant partner.

The NCB became operational in 1969 with a staff of three and an annual caseload of 300. Agents are complemented by computer specialists, analysts, translators, and administrative and clerical support personnel drawn largely from the ranks of the Department of Justice. The agents operate in divisions dedicated to specific investigative areas while the analysts review case information to identify patterns and links. The law enforcement agencies represented at the USNCB include the Bureau of Alcohol, Tobacco, and Firearms; the Drug Enforcement Administration (DEA); the Environmental Protection Agency; the FBI; the Financial Crimes Enforcement Network; the Fish and Wildlife Service; the Immigration and Naturalization Service (INS); Internal Revenue Service; U.S. Customs Service; the Department of Agriculture; the Department of Justice, Criminal Division; the Department of State; the U.S. Marshals Service; the U.S. Mint; the U.S. Postal Inspection Service; and the U.S. Secret Service. Additionally, each state, the District of Columbia, and New York City have established points of contact to receive international criminal reports from the NCB.

The USNCB operates by linking the Treasury Enforcement Computer System, the FBI's National Crime Information Center, the INS files, and the DEA records to Interpol. The international organization then funnels information from country to country. Classified information, including the vast majority of international terrorism cases, is not placed by the U.S. into Interpol channels because the flow of intelligence cannot be controlled and there are concerns that terrorists may tap into Interpol's intelligence system to plan strikes against the U.S. However, Interpol is utilized as a weapon against potential terrorists. The U.S. began accepting counter-terrorism cases in 1985. In 1990, the U.S. and Canadian governments established an Interpol Interface between the USNCB and the Canadian NCB in Ottawa. This link allows police to tap into law enforcement networks across the border to verify driver registrations and vehicle ownership.

The USNCB has grown considerably since its founding, responding to the increasing internationalization of crime as well as a jump in the numbers of foreign nationals entering the country. As these trends are likely to continue, the USNCB will likely see its crime fighting role increase in the future.



## ■ FURTHER READING :

### BOOKS:

Anderson, Malcolm. *Policing the World: Interpol and the Politics of International Police Co-operation*. Oxford: Clarendon Press, 1989.

Bresler, Fenton. *Interpol*. London: Sinclair-Stevenson, 1992.

United States Department of Justice and United States Department of the Treasury. *Interpol: The International Criminal Police Organization*. Washington, D.C.: Government Printing Office, 2002.

### SEE ALSO

*Classified Information*

*FBI (United States Federal Bureau of Investigation)*

*DEA (Drug Enforcement Administration)*

*Department of State, United States*

*INS (United States Immigration and Naturalization Service)*

*Internal Revenue Service, United States*

*Interpol (International Criminal Police Organization)*

*Justice Department, United States*

*Law Enforcement, Responses to Terrorism*

*Secret Service, United States*

*Treasury Department, United States*

## Interrogation

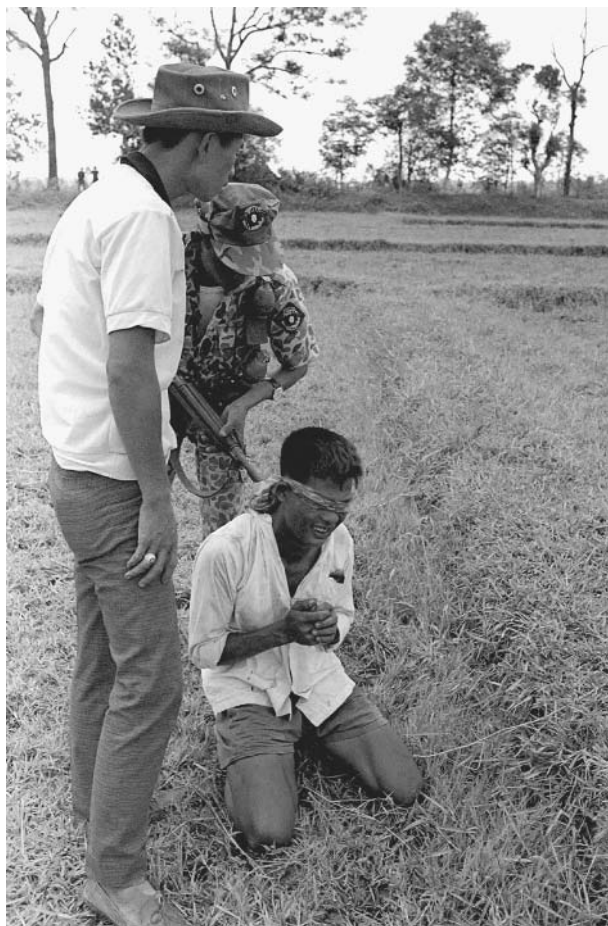
■ BRIAN HOYLE

Interrogation is a conversational process of information gathering. The intent of interrogation is to control an individual so that he or she will either willingly supply the requested information or, if someone is an unwilling participant in the process, to make the person submit to the demands for information. The latter can involve techniques of humiliation, intimidation, and fear. In more extreme cases in some countries, physical pain is inflicted.

Every interrogation is intended to strip away the subject's defenses and resilience. If the process is successful, the subject will eventually "give in" and supply the interrogator with the information being sought.

The interrogators hold much power in the interrogation process. By various techniques that are intended to manipulate the subject psychologically, the interrogator's aim is to dominate the subject. For example, an interrogator can display a great knowledge of the subject's background and actions. Whether or not the interrogator actually knows much about the subject is irrelevant. The point is to convince the subject that what the interrogator says is true, and so that resistance is pointless.

The surroundings are also an important part of the interrogation process. Often, as in a police station, jail, or clandestine hideaway, the conditions are foreign, Spartan, and even uncomfortable to the subject. This throws



A captured Viet Cong suspect found with a hidden automatic weapon during a "search and seal" operation is interrogated, South Vietnam, 1967. AP/WIDE WORLD PHOTOS.

the subject off balance. If the conditions are abruptly changed, as for example, being brought out of solitary confinement to be given a hot shower and a tasty meal, a subject's mood may change abruptly from despair to relief. Then, information may be offered to the interrogator out of gratitude.

During the early stages of an interrogation process, an interrogator will "get to know" the subject. It is important to find out whether a subject is, for example, zealously dedicated to a cause, to the point of becoming a martyr, or whether the subject needs little persuasion to become compliant.

A skilled interrogator will also observe a subject's physical posture and listen carefully to the tone of his or her voice, especially if behavior changes in response to some aspect of the conversation. For example, many people who are nervous or under stress will unconsciously and protectively draw their elbows in to their sides. As another example, when many people are talking about something they either know a lot about or are passionate about, their rate of speaking increases. But, if a subject

area is uncomfortable, many people pause and speak slowly. Knowing what topics a subject is sensitive to, and observing visual cues, can be used later as levers.

If a subject is reluctant to offer information, an interrogator will often begin to probe the topics that make the subject uncomfortable. By turns an interrogator can be calm or bluntly insistent. Both the topics discussed and the interrogator's manner are intended to keep the subject tense and off-balance, and to indicate to the interrogator how hard he or she may need to press to gain the information that is sought. A subject can become hostile during this phase of an interrogation, or may be compliant.

In the next phase of an interrogation process, the interrogator attempts to elicit the sought-after detailed information. The interrogator is firm and to the point at this stage, never allowing the conversation to stray off topic. The interrogator also will want to establish whether the subject's information is reliable. The interrogator can employ a variety of tactics, including leaving the subject alone for some time, making the subject think that he or she has no allies, using threats, talking about the subject's family, and even adopting a warm tone.

An interrogation is sometimes accomplished by a pair of interrogators, often with very different personalities. One person will be domineering, crass, profane, and loud. The other interrogator will be friendly, sympathetic, and quiet. This contrast, which is reinforced by a rehearsed routine, can work to the interrogator's advantage, particularly with women, teenagers, and shy people, who usually will respond to the quiet interrogator.

An interrogation can take place over days, with periods of solitary confinement in between. These solitary periods serve to build up tension in the subject and, especially if the surroundings are loud or uncomfortable, to make the subject exhausted.

As of late 2002, Amnesty International estimates that torture is part of interrogation in over 100 countries worldwide if a subject is especially uncooperative or displays great resiliency. Interrogation with torture may utilize drugs, hypnosis, threats of violence, and physical pain and injury to extract information.

## ■ FURTHER READING:

### BOOKS:

Elliston, Jon. *INTERRORgation: The CIA's Secret Manual on Coercive Questioning*, 2nd ed. San Francisco: AK Press, 1999.

Gordon, Nathan J., William L. Fleisher, and C. Donald Weinberg. *Effective Interviewing and Interrogation Techniques*. New York: Academic Press, 2001.

### SEE ALSO

*Interrogation: Torture Techniques and Technologies Language Training and Skills*

# Interrogation: Torture Techniques and Technologies

■ BRIAN HOYLE

Interrogation seeks to acquire information from a person. Since the person being interrogated is often not comfortable with the process or even willing to divulge information, the interrogation process is different from a conversation. Conversationally, information is freely exchanged and offered. However, interrogation is a less compliant process. Interrogation can take different forms, but these all have a similar aim: to control the subject in such a way that he or she yields to pressure and provides the information being asked for.

Information can be obtained by the use of pain. Torture is centuries old. In medieval times, as a few examples, victims were stretched on a rack, burned with hot branding irons, stoned, or uncomfortably shackled. But over the past century, techniques and technologies of physical and psychological torture have been "refined." Information can now be obtained without leaving a physical trace of the trauma of torture.

Newer methods of torture have been driven by the need for speed in obtaining the information, and, in the case of governments, in disguising the torture from organizations like Amnesty International that can hinder the information-gathering process.

## Torture Components

The techniques and technologies of torture can be grouped into three categories: hardware, software, and liveware. The term "hardware" refers to the equipment used; software refers to the techniques of torture that are taught to interrogators. Torture liveware refers to the human element of torture, typically the interrogator.

**Torture hardware.** Examples of torture hardware include shackles for the arms, legs, and even thumbs, whips, canes, beating devices (i.e., clubs, rubber hoses), water, electrical generators to administer electroshocks, and devices that suspend someone painfully above the ground. In fact, the list of physical harm that can be inflicted is long. Any possible route to inflict pain that can be conceived of has been used.

Machines that generate intolerable noise ("white noise") or bright pulses of ultraviolet light are sometimes used. Hardware can also have a chemical nature. Some drugs can cause physical discomfort, pain, and disruptions to the body's biochemistry. Examples include curare,



A British soldier stands in a room used for torture and interrogation in the Serbian military police headquarters in Pristina, 1999. Later, United Nations investigators examined the knives, wooden bats, brass knuckles, and drugs found in the building as part of a war crimes investigation. AP/WIDE WORLD PHOTOS.

insulin, and apomorphine. Drugs such as these differ from psychoactive drugs that alter thought processes or biochemical activity in the brain. Food and water deprivation, or maintaining an uncomfortable position for a long time, can also induce biochemical changes.

Electromagnetic radiation can also be a means of torture. Studies in animals have shown that electromagnetic waves of certain wavelengths can destroy lung and brain cells. While not necessarily lethal, these effects are debilitating and can be painful. Electromagnetic stimulation can have other nonlethal effects on humans. Extreme emotions of rage, lust, and fatigue can be caused. A 1950s research program called "Operation Knockout," which was funded by the United States Central Intelligence Agency, discovered that electroshock treatments could be used to cause amnesia. Memories could be erased, and the subjects reprogrammed. This "psychic driving" is a form of torture.

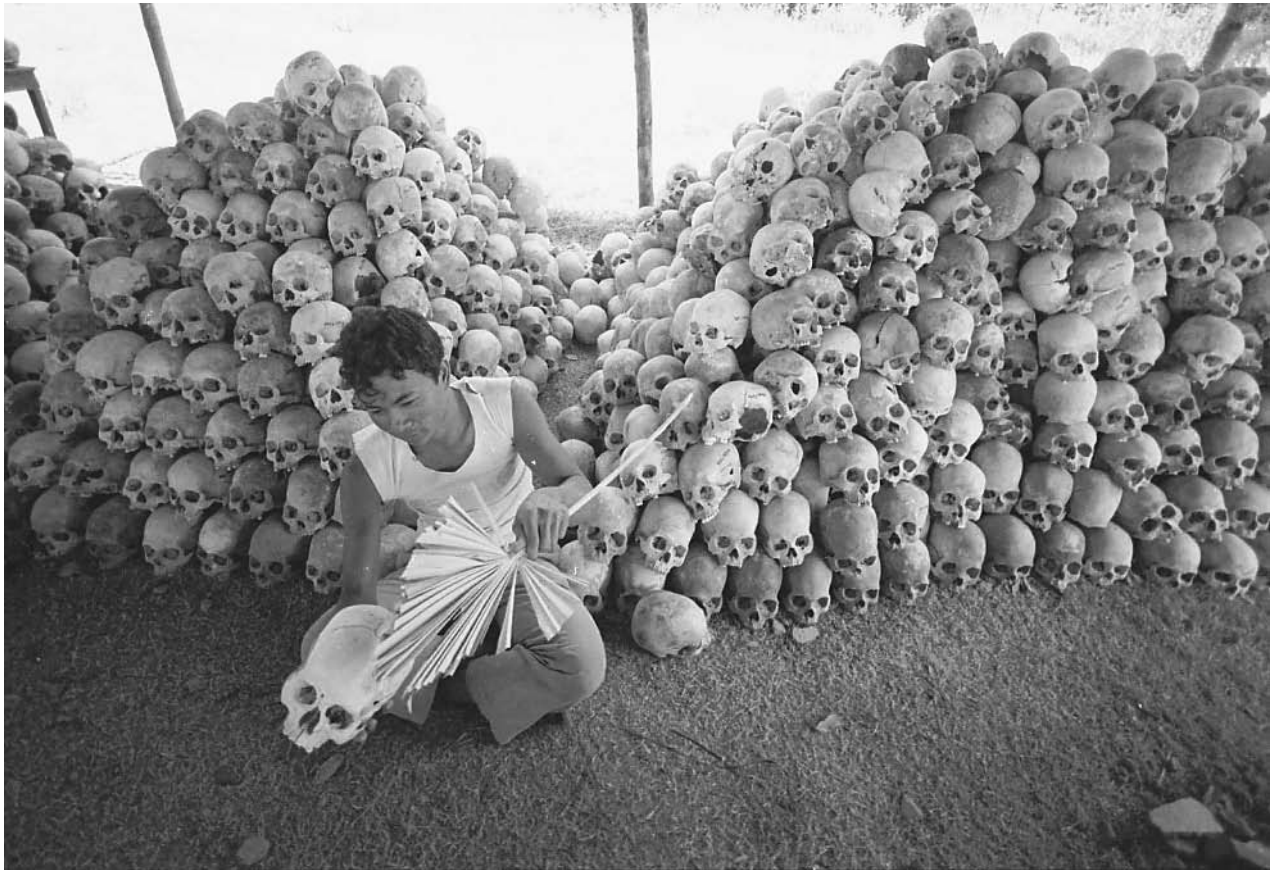
The most widely used torture hardware is electroshock. Pulses of energy, which are therapeutically useful in some medical treatments, have been adapted as a torture technique. The application of electricity stimulates muscle activity to such an extent that involuntary and

painful muscular contractions occur. Longer pulses of electricity produce successively greater debilitation. For example, a five-second discharge from a cattle prod can completely immobilize someone for up to 15 minutes

**Torture software.** The use of intimidation, threats, harsh and comforting language, and even silence are all techniques that, when combined with the hardware of torture, can extract information from a victim.

Such interrogation techniques have become standard operating procedures for interrogators. Indeed, manuals have been written for interrogators. One example is the *Human Resource Exploitation Training Manual*, which was written by the U.S. Central Intelligence Agency, and whose existence became known in 1997 as part of a Freedom of Information Request. A second example is the School of the Americas at Fort Benning, Georgia, which trained interrogators until 1991. The U.S. is by no means unique in providing such training.

**Technical and technological orchestration of torture.** Interrogation techniques are intended to "soften up" the victim,



A man cleans, numbers, and stacks skulls near a mass grave at the Cheung Ek torture camp run by the Khmer Rouge in Cambodia, where Pol Pot tortured and murdered between one and two million people to eliminate perceived opposition in the 1970s. AP/WIDE WORLD PHOTOS.

depleting the physical and mental resources that can be used to resist the pressure to reveal information. This is also known as breaking of the spirit. Depriving someone of sleep and sensory stimulation (by keeping them in a dark and soundless environment, akin to solitary confinement) can cause extreme anxiety, intense fear, and paranoia.

The behavior of the interrogator is an important part of the process. For example, a comforting word or supplying water and food can make a victim grateful enough to yield to a request for information. Conversely, degrading or demeaning behavior can cause the victim to give up.

Torture as practiced by terrorist organizations, military and paramilitary forces, and by other government agencies is seldom a haphazard affair. The task of breaking someone's spirit involves the coordination of activities, and the use of certain techniques and technologies at certain times.

The torture process can begin at the moment of arrest or kidnapping. Taking someone by surprise is more jarring than if someone has time to physically and mentally prepare himself or herself for arrest. The majority of people are at their lowest ebb both physiologically and

psychologically in the early morning or near bedtime. A surprise detainment at those times is especially jarring.

The feeling of disorientation and fear can be heightened during transport to wherever the victim is to be detained. For example, the use of a blindfold or a hood deprives someone of visual cues that can help them maintain a sense of control.

The next phase is usually detention. Time spent alone in unfamiliar surroundings, deprived of familiar and comfortable clothing, wondering about what is to come can be disorienting and terrifying. Also the detainee is forced to rely on his or her own mental resources, which can lead to self-doubt and fear.

Removing the stimuli for senses like sight and sound can be used during this and other phases of torture. Human physiology and behavior is largely governed by the input of information. If sensory stimulation is lacking, physical and mental deterioration often occurs. For example, a study was done where subjects were immersed in body-temperature water up to their necks. Their heads were hooded to blind them. After just a few hours, sensations of tension gave way to hallucinations.

Conversely, stimulating senses such as smell—by, for example, the lack of toilet facilities—can prove overwhelming.

The threat of torture can be as effective as the actual pain in destroying resistance. This is because many people are able to tolerate pain more so than they believe they can. Once the reality occurs, victims may even draw strength from their ability to withstand the torture. Once physical torture has begun, the threat of death can also help the victim. Indeed, death can be a welcome relief from the pain. If however, the torture is perceived as unending, information can be volunteered in the hopes of ending the suffering.

Pain is an inherent part of torture. Because people have different tolerances to pain, or are more sensitive to some forms of pain than to others, torture can be tailored to exploit the sensitivities of the victim.

The techniques and technologies of torture are pervasive and widespread. As newer technologies are developed for other humane purposes, it is likely that these will be adapted for the inhumane purpose of torture.

#### ■ FURTHER READING:

##### BOOKS:

Elliston, Jon. *INTERRORgation: The CIA's Secret Manual on Coercive Questioning, 2nd ed.* San Francisco: AK Press, 1999.

Gordon, Nathan J., William L. Fleisher, and C. Donald Weinberg. *Effective Interviewing and Interrogation Techniques.* San Diego: Academic Press, 2001.

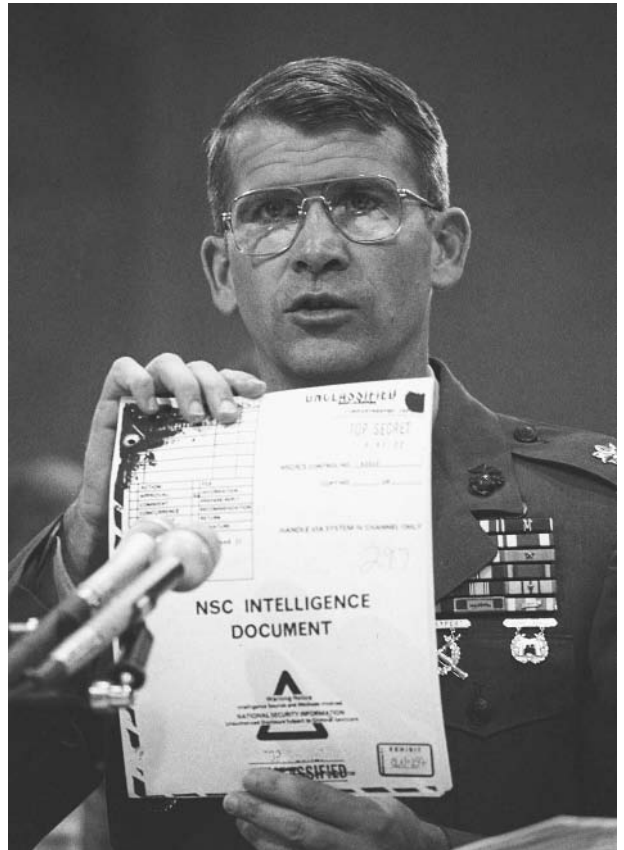
##### SEE ALSO

*Noise Generators*  
*Psychotropic Drugs*  
*Truth Serum*

## Iran-Contra Affair

#### ■ LARRY GILMAN

In October and November of 1986, it was discovered that for several years, agents of the United States government had been running an illegal operation to sell weapons to Iran and funnel the profits to the Contras, a military organization dedicated to overthrowing the leftist government of Nicaragua. In December, 1986, Lawrence E. Walsh was appointed independent counsel by the U.S. Court of Appeals for the District of Columbia Circuit. (An independent counsel is a prosecutor appointed by the Court of Appeals at the request of the Attorney General of the United States to investigate suspected crimes by members of the executive branch of government.) During the early phases of the investigation, a cover-up was attempted



Lt. Col. Oliver North holds up a National Security Council intelligence document marked "TOP SECRET" during testimony before the House-Senate investigating committee at the Iran-Contra hearings in Washington, D.C., 1987. AP/WIDE WORLD PHOTOS.

by the Reagan administration. In the words of Walsh's final report, "following the revelation of [the Iran-Contra] operations in October and November 1986, Reagan Administration officials deliberately deceived the Congress and the public about the level and extent of official knowledge of and support for these operations."

The Iran-Contra investigation lasted from 1986 to 1994. During this period, Walsh charged 14 Reagan Administration officials with criminal acts. He obtained convictions and guilty pleas in 11 cases. Two convictions were overturned on a technicality, and several officials, including Secretary of Defense Caspar Weinberger, were issued pre-trial pardons by President George H. W. Bush during the "lame duck" period following his electoral defeat in 1992. Walsh's investigation concluded that "the sales of arms to Iran contravened United States Government policy and may have violated the Arms Export Control Act," that "the provision and coordination of support to the Contras violated the Boland Amendment ban on aid to military activities in Nicaragua" (passed by Congress in 1984), and that "the Iran operations were carried out with the knowledge of, among others, President Ronald Reagan, Vice President George H. W. Bush, Secretary of

State George P. Schultz, Secretary of Defense Caspar W. Weinberg, and Director of Central Intelligence William J. Casey." Walsh did not have legal power to bring charges against President Reagan or Vice President George H. Bush, as the Boland Amendment was not a criminal statute containing specific enforcement provisions. Congress did not exercise its power to impeach.

**Historical background.** In 1979, the Somoza dictatorship in Nicaragua was overthrown by a left-wing revolutionary group calling itself the Sandinistas (after Nicaragua revolutionary leader Augusto César Sandino, 1893–1934). Soon after taking office in 1981, President Ronald Reagan ordered the Central Intelligence Agency (CIA) to secretly fund and equip the Contras, mostly former members of the Somoza military who sought the overthrow of the Sandinista government, and who were operating from bases in Honduras and Costa Rica (to the north and south of Nicaragua, respectively). On December 8, 1982, a bill was passed by the U.S. House of Representatives forbidding U.S. covert actions "for the purpose of overthrowing the government of Nicaragua;" some funding for the Contras was still allowed. Some of the Congressional reluctance to give U.S. support to the Contras arose from their unsavory tactics. As General John Galvin, commander of the U.S. Southern Command, testified to Congress, the Contras were directed by the CIA to "[go] after soft [i.e., undefended] targets . . . not to try to duke it out with the Sandinistas directly." In practice, this meant attacking medical clinics, schools, farmer's cooperatives, and other undefended elements of the civil infrastructure, causing almost exclusively civilian casualties.

In May, 1984, Congress discovered that its 1982 restrictions had been disregarded by the Reagan administration. CIA agents, acting at the behest of National Security Council member Oliver North, had been placing mines in Nicaraguan harbors despite the Congressional ban on such activities. Consequently, Congress cut off all funding for the Contras and passed the Boland Amendment, a statute prohibiting any U.S. agency involved in "intelligence activities" from "supporting, directly or indirectly, military or paramilitary operations in Nicaragua by any nation, group, organization or individual."

**The "Enterprise."** Direct and indirect support for the Contras continued in spite of the Boland Amendment, coordinated by Oliver North through a complex network he termed the "Enterprise." North's agents solicited money and arms for the Contras from three primary sources: (1) countries dependent on U.S. support, including South Africa, Brunei, Saudi Arabia, South Korea, and Israel; (2) wealthy Americans sympathetic to President Reagan's policies; and (3) weapons sales to Iran. The Reagan administration was secretly selling arms to Iran (in probable violation of the Arms Export Control Act of 1976, according to independent counsel Walsh); North's organization diverted money from these sales to the Contras. The

Contras also raised money by allegedly selling large quantities of crack cocaine in the United States with CIA complicity. All these activities violated the Boland Amendment's ban on aid to military activities in Nicaragua, as well as other laws.

Administration support of the Contras became public knowledge when a Contra military supply plane was shot down over Nicaragua on October 5, 1986. An American crew member, Eugene Hasenfus, was taken prisoner and revealed that he was a CIA agent. A month later, a Lebanese newspaper exposed the Reagan administration's secret sales of arms to Iran. On November 25, 1986, Justice Department officials went public with the information that these two news items were linked: proceeds from the Iranian arms sales has been diverted to the Contras.

At this stage, what independent counsel Walsh characterized in his official report as "a new round of illegality" began: "Senior Reagan administration officials engaged in a concerted effort to deceive Congress and the public about their knowledge of and support for the operations."

**Outcome of the investigation.** Fourteen officials were charged with criminal violations as a result of the Iran-Contra investigation. All individuals tried were convicted; one CIA official's case was dismissed because the government refused to declassify information needed for his defense; and two convictions were overturned on technicalities. A few of the most prominent persons charged, as described in the final report of the independent counsel, are listed below:

- (1) Elliott Abrams (Assistant Secretary of State for Inter-American Affairs): plead guilty to withholding information from Congress.
- (2) Robert C. McFarlane (National Security Advisor): plead guilty to four counts of withholding information from Congress.
- (3) Oliver L. North (Lieutenant Colonel, U.S. Marine Corps and Assistant Deputy Director for Political-Military Affairs of the National Security Council, 1981–1986): convicted of altering and destroying documents, accepting an illegal gratuity, and aiding and abetting in the obstruction of Congress.
- (4) John M. Poindexter (National Security Advisor): convicted of conspiracy, false statements, falsification, destruction and removal of records, and obstruction of Congress. Poindexter's conviction on all counts was overturned on appeal on the grounds that although he lied to Congress, he did so while speaking under a guarantee of immunity. Independent counsel Walsh noted in his final report that North's and Poindexter's convictions were "reversed on appeal on constitutional grounds that in no way cast doubt on the factual guilt of the men convicted."
- (5) Secretary of Defense Caspar W. Weinberger was charged with four counts of false statements and perjury. He was pardoned before trial by President George H. W. Bush, who also pardoned

Elliot Abrams, Robert McFarlane, and two other men at the same time.

**Aftermath.** The Iran-Contra affair, like the CIA-organized invasion of the Bay of Pigs in Cuba in 1961, struck a global blow to American credibility. Officials at the highest level had been detected organizing international terrorism (i.e., the Contras), violating U.S. law, and lying under oath. However, like that of the Bay of Pigs before it, the long-term impact of the Iran-Contra affair on U.S. politics and foreign policy was slight, and the central figures in the controversy later enjoyed high-profile careers in both the public and private sectors.

#### ■ FURTHER READING:

##### BOOKS:

Busby, Robert. *Reagan and the Iran-Contra Affair*. Chippenham, Wiltshire, Great Britain: Macmillan, 1999.

Marshall, Jonathan, Peter Scott, and Jane Hunter. *The Iran-Contra Connection*. Boston: South End Press, 1987.

##### ELECTRONIC:

Walsh, Lawrence E. "Final Report of the Independent Counsel for Iran-Contra Matters: Volume I: Investigations and Prosecutions." United States Court of Appeals for the District of Columbia, Division for the Purpose of Appointing Independent Counsel. August 4, 1993. <<http://www.fas.org/irp/offdocs/walsh/>> (December 10, 2002).

Webb, Gary. "Dark Alliance: The CIA, the Contras, and the Crack Cocaine Explosion." 2002. Originally published in San Jose Mercury News, 1996. <<http://home.attbi.com/~gary.webb/wsb/html/view.cgi-home.html-.html>> (December 10, 2002).

of Iran," the nation's "supreme leader" is a religious authority: first Khomeini and then, after Khomeini's death in 1989, Ayatollah Sayyed Ali Khamenei. The "supreme leader" sits on the Joint Committee for Special Operations, an Iranian organizational equivalent of the U.S. National Security Council.

Other members of the Joint Committee include the nation's president (its top secular official), and representatives of the Pasdaran, the Ministry of Foreign Affairs, and the Ministry of Security and Intelligence. The Joint Committee coordinates international activities of Iranian operatives, which include intelligence-gathering, attempts to obtain special weapons technology by clandestine means, and efforts to control the community of Iranian exiles—as well as alleged enemies of the revolution—overseas.

**VEVAK.** Iranian leaders' legendary hatred of the United States is rooted in history. The Central Intelligence Agency helped overthrow the government of Mohammad Mossadeqh in 1953, and provided support to his replacement, the Shah. U.S. and Israeli intelligence helped train the hated SAVAK, which included some 15,000 operatives and practiced torture using electric shock and other brutal methods. Ironically, when the new regime established its replacement for SAVAK—initially known as SAVAMA, and later retitled VEVAK—it needed experienced intelligence operatives, so it brought in former low-ranking officers of SAVAK and the Shah's military.

VEVAK operatives overseas use a number of covers, posing as bankers, students, laborers, or employees of Iran Air. These operatives help oversee an international terror network that claimed well over 1,000 lives in more than 200 terrorist attacks during the first two decades after the revolution. At times their work is assassination, as when they conducted a worldwide manhunt for author Salman Rushdie after the publication of his allegedly blasphemous 1989 novel *The Satanic Verses*.

In 1997, a German court convicted four assassins linked with Iran for the slaying of three Kurdish dissidents and their translator at a restaurant in Berlin in 1992. Much of the Iranians' operations in Germany took place through their diplomatic mission, from which they monitored some 100,000 Iranian expatriates throughout the country. Iran also used its diplomatic mission as cover for efforts to procure nuclear, chemical, and biological weapons technology.

Iranian and Iranian-sponsored terrorists have been involved in an array of worldwide terrorist activities including: the bombing of the U.S. Marine barracks in Beirut, Lebanon, in 1983; bombings in Paris in 1986; at the Israeli embassy and a Jewish community center in Buenos Aires in 1992 and 1994; and at Dhahran, Saudi Arabia, in June 1995. Following the terrorist attacks of September 11, 2001, President George W. Bush labeled Iran, Iraq, and North Korean "Axis of Evil" in his 2002 State of the Union speech.

## Iran, Intelligence and Security

Iran has a number of intelligence and security organizations that include the Ministry of Intelligence and Security (known as VEVAK for its initials in Farsi), as well as the group called the Pasdaran, or Guardians of the Islamic Revolution. Up to 1978, Iran was controlled by Shah Mohammed Reza Pahlevi, who maintained power through a state security organization, SAVAK. His overthrow led to the establishment, in 1979, of the world's first major Islamic theocracy under the Ayatollah Ruhollah Khomeini. Thus was born a new form of police state in contrast to the Soviet, Nazi, or nationalist models—a state in which security forces are often directed toward the enforcement of religious law.

In accordance with the theocratic nature of government in a country officially known as "the Islamic Republic

**The Pasdaran.** Western analysts argue that sponsorship of terror in the name of Islam is one of the few things Iran has in common with Iraq, against which it fought what became the longest and bloodiest war anywhere in the world since WWII. Among the notable aspects of the grisly 1980–88 Iran-Iraq war were the *Bajeef* (volunteers), young men without military training who volunteered to go to the front on suicide missions. After the war, they were incorporated in a larger force that had existed since May 1979, when Khomeini established it by decree: the Pasdaran.

Former Bajeef members, and other Pasdaran with lower levels of training, were detailed to perform the functions of a theocratic police force—harassing or arresting women who wore makeup or inappropriate attire, and seizing forbidden items such as videotapes, photographs, pork products, and alcohol. At the more sophisticated end of Pasdaran operations are its activities overseas, including those of the Qods or Jerusalem Force, which in the mid-1990s allegedly trained terrorists in Sudan and elsewhere.

**Exporting the revolution.** Iran sought to export its revolution through support of Sh'ia Muslim factions such as Hizballah in Lebanon, but its leadership did not necessarily resist alliances with Muslims of the larger Sunni sect. Hence, during the mid-1990s Iran sought to build ties with Bosnia—ironically, a country known in the West for the relative moderation of its Muslims. Still, Iran succeeded in placing several hundred agents in Bosnia, where they even penetrated U.S. efforts to train the Bosnian army.

Another branch of the Pasdaran consisted of some 12,000 Arabic-speaking operatives of many nationalities working with Hizballah, Kurdish groups, and other armies in central Asia. In a particularly stunning example of the continued international flavor of terrorism, the Pasdaran “Operation of Liberation Movements” attended a coordination meeting in Beirut in April 1995 with representatives of Hizballah, the Iraqi Da'Wah Party, the Islamic Front for the Liberation of Bahrain, the Kurdistan Workers' Party, the Armenian Secret Army, and the Japanese Red Army.

#### ■ FURTHER READING :

##### BOOKS:

Daughtery, William J. *In the Shadow of the Ayatollah: A CIA Hostage in Iran*. Annapolis, MD: Naval Institute Press, 2001.

Roosevelt, Kermit. *Countercoup, the Struggle for the Control of Iran*. New York: McGraw-Hill, 1979.

##### PERIODICALS:

Karmon, Ely. “Counterterrorism Policy: Why Tehran Stops and Starts Terrorism.” *Middle East Quarterly* V, no. 4 (December 1998).

Samii, Abbas William. “The Shah’s Lebanon Policy: The Role of SAVAK.” *Middle Eastern Studies* 33, no. 1 (January 1997): 66–91.

##### ELECTRONIC:

Iran—A Country Study. Library of Congress. <<http://lcweb2.loc.gov/frd/cs/irtoc.html>> (March 26, 2003).

Iran-e-Azad: Supporters of the National Council of Resistance of Iran. <<http://www.iran-e-azad.org/english/index.html>> (March 26, 2003).

Iranian Intelligence Agencies. Federation of American Scientists. <<http://www.fas.org/irp/world/iran/index.html>> (March 26, 2003).

##### SEE ALSO

*ADFGX Cipher*  
*European Union*  
*Iran-Contra Affair*  
*Iranian Nuclear Programs*  
*Iraq, Intelligence and Security Agencies*  
*Khobar Towers Bombing Incident*

## Iranian Hostage Crisis

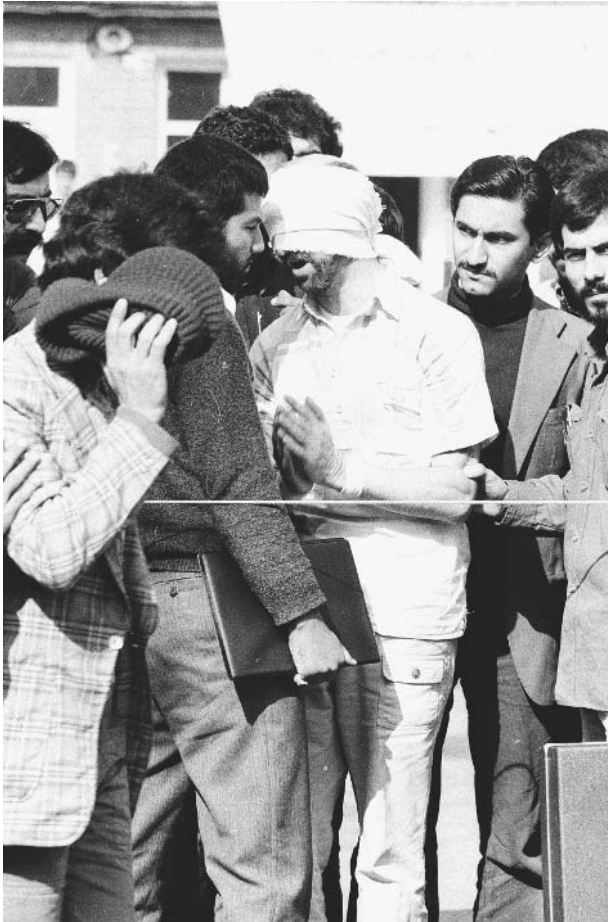
■ STEPHANIE WATSON

On November 4, 1979, a group of Iranian militants stormed the American embassy in Tehran, Iran, and captured dozens of embassy and military personnel. For 444 days, fifty-two Americans remained captive in Iran, while their nation waited, hoped, and hung yellow ribbons. The outcome of the hostage crisis would ultimately change the course of a presidency, and malign relations between two powerful nations.

**The origins of anti-American fervor.** In the early 1970s, America and Iran enjoyed mutually satisfying relations. At the time, the country was ruled by Shah Mohammad Reza Pahlavi, a man the American government had supported for more than twenty-five years. Pahlavi had risen to power thanks to British and Soviet forces, which jointly installed Pahlavi on the throne in 1941 to gain valuable influence over the country’s oil. Two years later, the United States and Great Britain made a formal declaration to promote Iran’s independence, primarily to prevent the communists from gaining a strong foothold in the country.

In the early 1950s, the Iranian prime minister, Mohammad Mossadegh, began gaining power and public support, and vehemently opposed the western influence in Iran. In 1952, Mossadegh’s party won the national elections, and he demanded control over Iran’s armed forces, which Pahlavi denied. In 1953, the United States Central

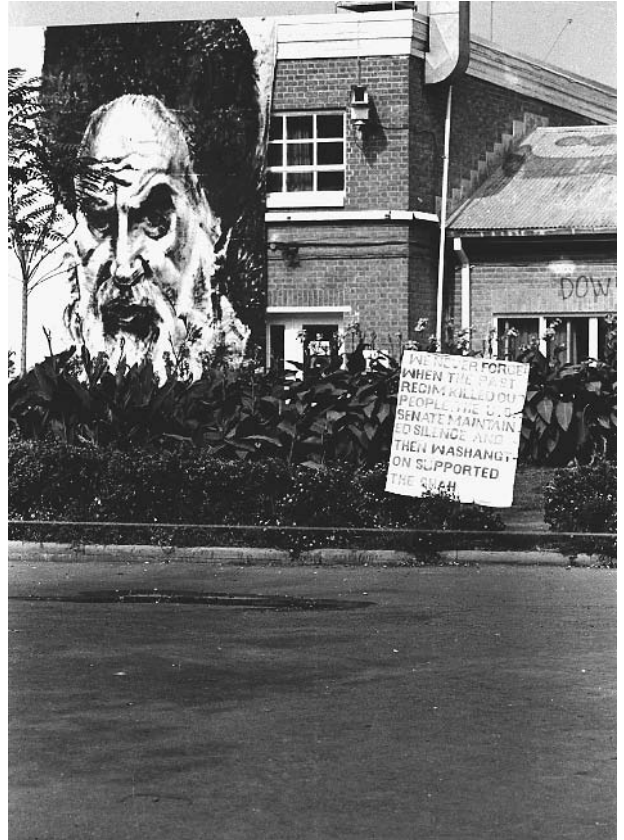




Blindfolded and with his hands bound, an American hostage is led by young militants in front of the United States Embassy in Tehran, November 8, 1979. AP/WIDE WORLD PHOTOS.

Intelligence Agency (CIA) secretly helped to overthrow Mossadegh and restore Pahlavi to power. Pahlavi remained a friend to the United States, but endured harsh criticism by his countrymen for ruling with an iron fist, and living opulently off the spoils of his country's oil production while the majority of his people lived in poverty. During the next two decades, the Shah attempted to bring further Western influence to Iran, a practice that was an anathema to the growing numbers of fundamentalist Islamic groups in the country. Those who dared oppose the Shah's rule faced the risk of torture or death at the hands of his secret police.

In 1978, Iranian opposition leaders organized strikes, demonstrations, and riots in protest of the Shah's policies. In Paris, exiled Islamic leader Ayatollah Ruhollah Khomeini (Pahlavi had sent Khomeini from the country amid riots in the early 1960s) slowly began to gain popularity among the Iranian people. In December, 1978, Khomeini issued a proclamation calling for Iranians to "unite, arise, and sacrifice your blood," urging them to defy the Shah's order prohibiting public demonstrations. Khomeini's words



A portrait of Iranian leader Ayatollah Khomeini hangs from the roof inside the compound of the United States Embassy in Tehran. AP/WIDE WORLD PHOTOS.

inspired his followers to fill the streets, chanting religious slogans and calling for revolution. The Shah was left with two choices: surrender or clamp down on his people militarily to restore order. On January 16, 1979, the Shah stepped down from power and fled to Morocco.

Khomeini returned to Iran on February 1, 1979, where he was greeted by millions of his followers. Less than two weeks later, Khomeini assumed power, announcing the creation of a new fundamentalist Islamic state. Khomeini labeled the United States "The Great Satan." Hatred grew when U.S. President Jimmy Carter allowed the deposed Shah to travel to America later that year for cancer treatment. Furious students gathered in the streets, raising their fists and shouting, "Death to America," assuming the United States was again trying to secretly restore the Shah to power.

On the morning of November 4, 1979, Iranian fervor reached a boiling point. A crowd gathered around the U.S. embassy, shouting anti-American slogans. At 10:30 A.M. about three thousand people jumped the ten-foot wall surrounding the embassy and swarmed the grounds, forcing their way into the basement and first floor of the chancery building. The guards launched tear gas, but they were unable to control the mob. The Islamic militants

rounded up 66 embassy workers, military officials, and Marine guards. The hostages were blindfolded, bound, and shoved into windowless rooms. Fifty-three people were held captive in the embassy compound. It was unclear what role, if any, Khomeini played in orchestrating the hostage crisis, but it was clear that he did little to stop it. When Khomeini noted how popular the hostage situation had become among his people, he allowed it to continue, despite continuous pressure from the United States government.

Americans watched the events of the crisis played out on television. Yellow ribbons were tied around tree trunks throughout the country in commemoration of the hostages. President Carter responded by freezing billions of dollars in Iranian assets, both in the United States and abroad, and by instituting an embargo on Iranian oil. Still, the Iranians refused to release the hostages, demanding the Shah's extradition to Iran.

**A rescue attempt.** While President Carter was trying to negotiate the hostages' release, behind-the-scenes a daring rescue plan was taking shape. The proposal was to swoop in and land eight American military helicopters in the embassy compound, extract the hostages, and escape to six planes waiting on an airstrip in the Iranian desert. On April 24, 1980, the plan was launched. The mission, however, was fraught with mistakes and bad luck. Three of the helicopters malfunctioned; the pilot of a fourth, blinded by a dust storm, crashed into a refueling aircraft. Eight U.S. servicemen were killed in the unsuccessful operation.

The hostage-takers responded to the failed rescue attempt by moving their captives to several secret locations in different cities. On July 11, one ill captive was released. Meanwhile, the ongoing hostage crisis was costing President Carter the support of his people and some of his advisors, including Secretary of State Cyrus Vance, who had opposed the rescue. Carter later lost his reelection bid to former California governor Ronald Reagan in a landslide.

**The siege ends.** In the fall of 1980, the exiled Shah died of cancer complications. In September, Iran agreed to begin negotiations for the hostages' release. In exchange for their release, the United States agreed to turn over \$8 billion of Iran's frozen assets, and to refrain from interfering politically or militarily in Iran's internal affairs. The United States and Iran signed the agreement on January 19, 1981, but in a final embarrassment to Carter, the militants did not release the hostages until January 20, the day President Reagan was inaugurated. Just minutes after Reagan took office, a plane carrying the fifty-two remaining hostages left Tehran for a U.S. Army base in Germany. From his home in Georgia, former president Carter announced that the plane carrying the hostages had cleared Iranian airspace, and that every one of the hostages "was alive, was well, and free."

## ■ FURTHER READING:

### BOOKS:

Rivers, Gayle, and James Hudson. *The Teheran Contract*. Garden City, New York: Doubleday & Company, Inc., 1981.

Sick, Gary. *All Fall Down: America's Tragic Encounter with Iran*. New York: Random House, Inc., 1985.

Wells, Tim. *Four Hundred and Forty-Four Days: The Hostages Remember*. Orlando, Florida: Harcourt Brace Jovanovich Publishers, 1985.

### PERIODICALS:

Schaumburg, Ron. "Americans Held Hostage." *New York Times Upfront*. (January 15, 2001):23.

Olson, Tod. "America Held Hostage: The Iranian Hostage Crisis Would Torment America—and Topple a President." *Scholastic Update*. (May 11, 1998):20–22.

### SEE ALSO

*Carter Administration (1977–1981), United States National Security Policy*  
*Iran, Intelligence and Security*

---

## Iranian Nuclear Programs

---

### ■ K. LEE LERNER

In his 2002 State of the Union speech, United States President George W. Bush labeled Iran, Iraq, and North Korea as rogue nations that constituted an "axis of evil" seeking to develop weapons of mass destruction (i.e., nuclear, chemical, or biological weapons).

Late in 2002, reports began to circulate in the press that Iran had taken steps to accelerate an already active nuclear program that could develop nuclear weapons. As a signatory to the Non-Proliferation Treaty, Iran has a right to pursue nuclear technology for peaceful purposes, subject to oversight by the International Atomic Energy Agency (IAEA). A development of nuclear weapons by Iran, however, would violate nuclear non-proliferation treaties.

Initial reports of Iranian nuclear program development by the National Council of Resistance of Iran, a private group that paid for their own intelligence estimates—including satellite imagery—gained influence because of the group's track record about supplying verifiable and reliable information regarding Iran's nuclear program. Western intelligence agencies soon confirmed the validity of the physical evidence of activity at Iranian nuclear facilities.

In December, U.S. State Department spokesman Richard Boucher argued that satellite imagery depicting the covering of buildings at the Natanz site indicated that Iran was building "a secret underground site where it could produce fissile material."

Iran quickly denied any attempt to develop nuclear weapons of mass destruction. Iranian officials asserted that the building programs underway at the suspected facilities were designed to expand Iran's ability to produce electrical energy. In particular, Iranian officials denied that its first nuclear plant—a reactor facility under construction at Bushehr, an Iranian town near the Persian Gulf Coast—would be equipped to produce weapons grade uranium. Iran's development of the facility at Bushehr (allegedly a 1,000-megawatt reactor) was supported by equipment and technical assistance from Russia.

In January, 2003, Iran announced its intention to develop a nuclear fuel program. Iran announced the mining of uranium and the adaptation of facilities, including the Natanz nuclear facility under construction, so that they could process ore into fissionable fuel for nuclear power plants. Iranian opposition groups and Western intelligence services argue that the nuclear fuel program could easily be extended to produce weapons grade fuel. The Iranian decision to produce its own fuels was chilling to Western intelligence services because it would eliminate the protections afforded by Russian demands to return spent fuel initially supplied for Iranian reactors.

Although Russian sales and support of nuclear materials and reactor equipment to Iran was well known, evidence of additional international interests in the Iranian program surfaced when the National Council of Resistance of Iran provided evidence that Chinese nuclear scientists and engineers were sighted at a uranium mine near Saghand. Chinese and North Korean scientists and engineers were reportedly involved in the development of uranium enrichment capability at a site near Isfahan. There were also allegations of centrifuge facility construction near Tehran.

The events in Iran signaled a change in the pace of Iranian nuclear program development that might allow Iran to construct an operational nuclear weapon by 2004 or 2005.

Concerned that Iran was attempting to accelerate its nuclear programs in such a way as to facilitate nuclear weapon development—especially while world attention was focused on events in Iraq and North Korea—IAEA inspectors requested additional access to inspect Iranian facilities. IAEA requests were initially denied. Iranian officials also initially declined to elaborate the intended uses of a facility in Khashan.

In February, 2003, IAEA inspectors, including IAEA chief inspector Mohamed El Baradei, were permitted to visit several new Iranian nuclear sites suspected of being able to enrich uranium for potential weapons use. Inspectors were also to make inquiries regarding the status of processing equipment located at Natanz and Arak (a heavy-water production facility) and to ask Iranian officials to accept regular monitoring of Iranian nuclear programs.

Satellite imagery indicated buried facilities near Natanz, and ground-based reports indicated the assembly of more than 150 centrifuges near the Natanz facility

nearing operational capability to process uranium gas into nuclear fuel capable of undergoing fission. Parts for additional facilities were also reportedly near the Natanz site. Iran admitted to IAEA officials the construction of a plant to convert uranium into UF<sub>6</sub> (uranium hexafluoride)—a gaseous form of uranium used in centrifuges.

Western intelligence scientists and analysts predicted that if Iran built its projected 5000 centrifuges, it could produce enough fuel each year for several nuclear weapons. United States officials briefed on IAEA reports from Iran expressed surprise at the advanced state of Iranian nuclear development. Several officials described Iran as being years ahead of prior projections and much closer to having nuclear weapons capability than previously estimated.

The United States has imposed sanctions against Russian companies and attempted to exert diplomatic pressure on Russia, Ukraine, and China, in an effort to prevent Iranian acquisition of sensitive nuclear technologies and equipment. Despite these efforts, intelligence sources predict that Iran's current nuclear program infrastructure will soon support the development of uranium-based weapons.

#### ■ FURTHER READING:

##### PERIODICALS:

Dareini, Ali A. "U.N. Nuclear Chief Arrives in Iran to Visit Nuclear Facilities." *The Washington Post*. February 21, 2003.

Kessler, Glenn. "Group Alleges New Nuclear Site in Iran." *Washington Post*. February 20, 2003.

Warrick, J., and G. Kessler. "Iran's Nuclear Program Speeds Ahead 'Startling' Progress at Complex Poses Challenge to Bush Administration at Delicate Time." *Washington Post*. March 10, 2003.

##### SEE ALSO

*Air Plume and Chemical Analysis*  
*Iran, Intelligence and Security*  
*Nuclear Detection Devices*  
*Nuclear Reactors*  
*Nuclear Weapons*

---

## Iraq, Intelligence and Security Agencies in

---

■ K. LEE LERNER

Prior to Operation Iraqi Freedom, under the rule of Saddam Hussein, the intelligence and security agencies of Iraq, commonly referred to as the *Mukhabarat*, included the General Intelligence Directorate (GID), Amn al Amm, Special Security Service (SSS), Fedayeen Saddam (named

after the Iraqi dictator, Saddam Hussein), Murafaqin, and Al Hadi.

The GID was tasked to collect and analyze foreign and domestic intelligence. The GID operated under state security officers and utilized a staff of nearly 4,500 intelligence officers and operatives. Following the Persian Gulf War, until weapons inspectors were expelled by Iraq in 1998, GID personnel often acted as “minders” for United Nations weapons inspectors and were tasked with both developing intelligence regarding inspector activities and with carrying out disinformation events designed to thwart inspector’s efforts to identify prohibited weapons.

In 1993, American forces launched an attack using Tomahawk cruise missiles that destroyed GID headquarters in retaliation for a failed Iraqi attempt to assassinate former United States president George H. W. Bush during his visit to liberated Kuwait.

The Amn al Amm (also known as the General Security Service) functioned as a secret police force under the control of the Iraqi Security Directorate. Amn al Amm personnel were tasked with spying on Iraqi citizens to ensure loyalty to Hussein’s regime—and to prevent anti-government rebellions from organizing. Amn al Amm officers were integrated into local police units throughout Iraq. A good deal of Amn al Amm’s operations were devoted to developing and maintaining extensive files on Iraqi citizens.

The Amn al Khas (also known as the Special Security Service or Presidential Affairs Service) was under the direct control of one of Hussein’s sons, Qusay Hussein. Under the close and brutal control of Qusay, Amn al Khas contained highly motivated Ba’thist party members who were intensely loyal to the Hussein family and served as Hussein family bodyguards. Following the Persian Gulf War, Qusay directed Amn al Khas troops in the hiding of biological and chemical weapons of mass destruction. U.N. weapons inspectors were continually thwarted by Amn al Khas personnel to the extent that the U.N. weapons inspectors failed to find evidence of Iraq’s extensive biological weapons program (e.g., anthrax production) until they received information following the 1995 defection of Hussein Kamil, Saddam’s son-in-law. Kamil was later lured back to Iraq by promises of leniency, and, despite the pleas of Saddam’s daughter, who was married to Kamil, he was tortured and executed.

Qusay Hussein reportedly directed Amn al Khas personnel in the vicious suppression of a rebellion by Shi’a groups in southern Iraq who led a failed rebellion against the Hussein regime following the Persian Gulf War. Qusay’s troops also directly controlled Iraq’s chemical weapons program and arsenal.

The Fedayeen Saddam (translated as Men of Sacrifice) was a group of zealous paramilitary thugs and criminals under the control of Saddam’s son Uday Hussein. Qusay was also known to exercise control over the Fedayeen during some operations. Numbering nearly 40,000 troops, the irregular Fedayeen forces carried out

harassment operations against U.S. led coalition forces and supply lines during Operation Iraqi Freedom.

Murafaqin (Companions of Saddam) security personnel were composed of Hussein’s al Bu Nasir tribal kinsmen. They acted as a protective secret service for the Hussein family—and often contributed guards assigned to physically protect Hussein family members.

The Al Hadi, also known as Department 858 or Project 858, functioned as Iraq’s signals intelligence (SIGINT) and electronic intelligence (ELINT) service under Hussein’s rule.

Qusay Hussein and his brother Uday were killed in a firefight with U.S. forces on July 22, 2003.

#### ■ FURTHER READING:

##### PERIODICALS:

Marashi Ibrahim al-. “Iraq’s Security and Intelligence Network: A Guide and Analysis,” *Middle East Review of International Affairs* 6, no.3 (September, 2002).

---

## Iraq War: Prelude to War (The International Debate Over the Use and Effectiveness of Weapons Inspections)

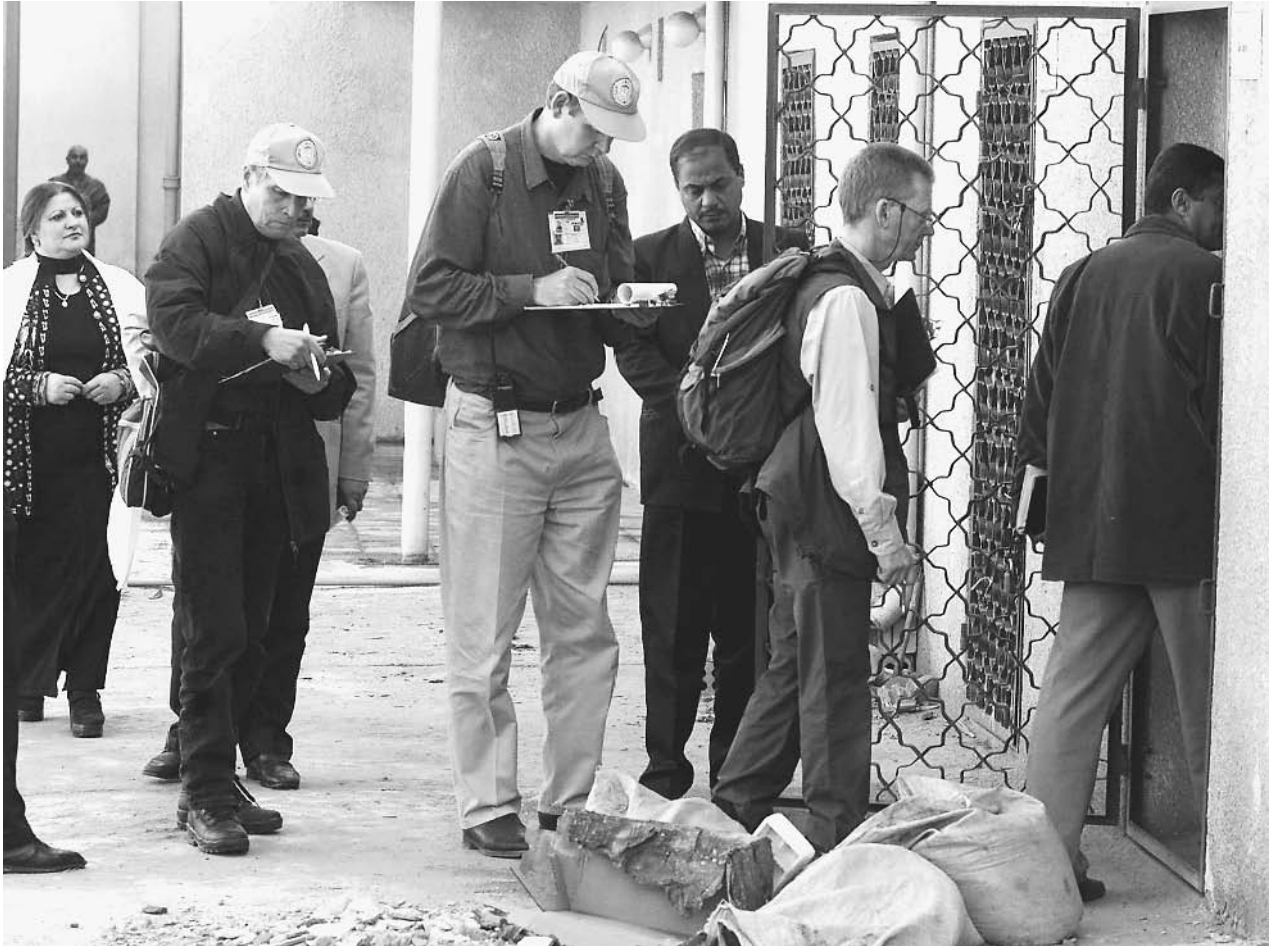
---

■ K. LEE LERNER

In the aftermath of the September 11, 2001, terrorist attacks on the United States and the subsequent war against the Taleban and al-Qaeda in Afghanistan, United States leaders turned their attention to an old enemy, Iraq, and specifically its dictatorial leader, Saddam Hussein.

Although Iraq was not as powerful a military threat as during the Persian Gulf War of 1990–1991, U.S. officials asserted that Iraq’s proven development and use of weapons of mass destruction made Iraq a potential source of those weapons for terrorists who could then use them against U.S. or other Western targets. Hussein ordered the use of chemical weapons against Iranian forces during the 1980s Iran-Iraq War, and additionally used chemical weapons against civilians in rebellious area of Iraq.

After Iraqi forces were expelled by U.S.-led Western coalition forces during the Persian Gulf War, and as a part of the agreements that prevented the occupation of Iraq and allowed Hussein to remain in power, Hussein agreed to destroy all weapons of mass destruction and forsake



In their trademark blue caps, United Nations weapons inspectors take notes during a visit to a veterinary research center in Baghdad, January 9, 2003. ©AFP/CORBIS.

the future development of nuclear, biological, and chemical weapons. During the next decade, however, 17 specific United Nations Security Council resolutions, weapons inspection programs, and economic sanctions against Iraq failed to secure Hussein's full compliance and assure disarmament of such weapons.

U.S. officials offered prior UN weapons-inspector declarations of Iraqi compliance as proof that Hussein was able to deceive inspectors. Discovery of Iraqi nuclear weapons development facilities in the early 1990s invalidated declarations by IAEA chief Hans Blix that Iraq had no viable nuclear weapons program. After dismantling the Iraqi nuclear program, weapons inspectors had also failed to uncover Iraqi biological and chemical weapons facilities until information supplied to Western intelligence sources by the defection of a son-in-law of Hussein (later executed by Hussein when he returned to Iraq) provided evidence of biological and chemical weapons programs.

Although many weapons were subsequently discovered and destroyed by inspection teams, Iraqi defiance of UN resolutions continued throughout the 1990s. The United

Nations Monitoring, Verification and Inspection Commission (UNMOVIC) was created by the UN Security Council (resolution 1284) in December, 1999. UNMOVIC was chartered to replace the former UN Special Commission (UNSCOM) and continue the mandate to disarm Iraq of its weapons of mass destruction and monitor compliance with other UN stipulations (e.g., that Iraq not possess missiles with a range of more than 150 km). Blix was named the commission's executive chairman. UNMOVIC staff included weapons specialists, scientific analysts, engineers and operational planners. In 1998 Iraq expelled the weapons inspectors and no meaningful inspections took place between 1998 and 2002.

Some Pentagon and administration officials urged immediate and direct action be taken by the United States to disarm Iraq. There were also more controversial calls for a "regime change" in Baghdad as the only means to assure Iraqi disarmament. United States President George W. Bush decided instead to seek international cooperation to disarm Iraq. In September 2002, Bush addressed the United Nations and called for a strong resolution that,

backed by the threat of the use of military force, would assure that Iraq possessed no weapons of mass destruction. In October 2002, the U. S. Congress voted Bush the authority to use military force to enforce UN resolutions.

In November 2002, the United Nations Security Council unanimously passed resolution 1441 that reiterated Iraq's obligations to disarm in accordance with prior treaty and resolution obligations and further recognized the threat that "Iraq's non-compliance with Council resolutions and proliferation of weapons of mass destruction and long-range missiles poses to international peace and security." Resolution 1441 went on to restate Security Council intentions to "restore international peace and security in the area."

Resolution 1441 specifically stated that Iraq "has not provided an accurate, full, final, and complete disclosure...of all aspects of its program to develop weapons of mass destruction and ballistic missiles with a range greater than one hundred and fifty kilometers, and of all holdings of such weapons, their components and production facilities and locations, as well as all other nuclear programs, including any which it claims are for purposes not related to nuclear-weapons-usable material."

Resolution 1441 additionally stated that Iraq had "repeatedly obstructed immediate, unconditional, and unrestricted access to sites designated by the United Nations Special Commission (UNSCOM) and the International Atomic Energy Agency (IAEA), [and had] failed to cooperate fully and unconditionally with UNSCOM and IAEA weapons inspectors...." The resolution deplores "the absence, since December 1998, in Iraq of international monitoring, inspection, and verification, as required by relevant resolutions, of weapons of mass destruction and ballistic missiles, in spite of the Council's repeated demands that Iraq provide immediate, unconditional, and unrestricted access to the United Nations Monitoring, Verification, and Inspection Commission (UNMOVIC), established in resolution 1284 (1999) as the successor organization to UNSCOM, and the IAEA...."

Important to U.S. concerns regarding potential links between Iraq and terrorist organizations, resolution 1441 recognized that Iraq had "failed to comply with its commitments pursuant to resolution 687 (1991) with regard to terrorism, pursuant to resolution 688 (1991) to end repression of its civilian population and to provide access by international humanitarian organizations to all those in need of assistance in Iraq...." Important to questions of legitimacy regarding potential military action against Iraq, resolution 1441 recalled "that in its resolution 687 (1991) the Council declared that a ceasefire [of the Persian Gulf War] would be based on acceptance by Iraq of the provisions of that resolution, including the obligations on Iraq contained therein."

Resolution 1441 declared Iraq to be in material breach (a violation of an important or substantial issue, not just a violation of a technicality or legal process issue) of prior resolutions and set out specific demands for Iraq including

resumption of inspections in Iraq by UNMOVIC and the IAEA based upon a full and truthful declaration of prohibited weapons (e.g., chemical weapons, biological weapons, nuclear weapons, nuclear programs, ballistic missiles, and prohibited weapons delivery systems).

Resolution 1441 specifically warned Iraq that future false statements or omissions in the declarations submitted by Iraq would constitute "a further material breach of Iraq's obligations" and reiterated the Security Council's warnings that "Iraq will face serious consequences as a result of its continued violations of its obligations."

In December, 2002, Iraq produced a 12,000-page document on its weapons programs. U.S. and U.K. officials declared the declaration false, and subsequently, UN weapons inspection teams argued that the document contained little in the way of new information and that it failed to signal Iraq's willingness to cooperate with the international community. Weapons inspectors from UNMOVIC and IAEA returned to Iraq in December 2002.

In late January, Blix, now the chief UNMOVIC weapons inspector, delivered what many observers concluded was a negative report on Iraq's cooperation with the latest in a twelve-year string of UN resolutions to disarm. Blix's report to the Security Council stated, "Iraq appears not to have come to genuine acceptance—not even today—of the disarmament which was demanded of it and which it needs to carry out to win the confidence of the world and live in peace." Blix went on to specifically cite Iraqi failures to eliminate prohibited chemical and biological arms programs.

Mohamed El Baradei, the IAEA chief inspector for atomic weapons, reported that Iraq had apparently been unable to successfully reconstitute its nuclear weapons program. Although there was disputed evidence that Iraq continued to try to obtain elements of nuclear weapons, it became apparent to inspectors that the destruction or dismantling of Iraq's nuclear program in the early 1990s had prevented Iraq from successfully developing nuclear weapons. Prior to the first Gulf War and the subsequent dismantling of equipment by UN forces, Western intelligence analysts estimated that without intervention, Iraq had been within two years of developing operational nuclear weapons. Based upon El Baradei's report, attention quickly focused on Iraq's chemical and biological weapons program.

Iraq rejected all of the inspectors' negative comments and the Iraqi ambassador, Mohammed A. Aldouri, insisted that Iraq had "fully complied with all its obligations" with regard to UN resolution 1441, which required disclosure of weapons and disarmament by Iraq.

Repeating a stand carefully articulated prior to the passage of UN 1441, President Bush reiterated U.S. resolve to disarm Iraq by force if necessary—even without support by other United Nations Security Council members with veto power (France, Russia, China). The other country with veto power, the United Kingdom, sided with the United States. At peril to their political futures, U.K.

Prime Minister Tony Blair and Home Secretary Jack Straw (their own Labour party remained deeply divided over the use of force to disarm Iraq) carefully articulated both the strategic need to prevent Iraq from becoming a conduit through which terrorists could obtain weapons of mass destruction, and also of the humanitarian need to liberate the Iraqi people from the despotic rule of Saddam Hussein. Veto-bearing Security Council members (i.e., France, Russia and China)—joined by members Germany and Syria—contended that the inspections process was yielding results and that additional time should be allowed for Iraq’s disarmament.

In statements and reports, Blix’s inspection team reported that despite Iraq’s denials, there were indications that Iraq had created weapons of mass destruction, including VX agent, a weapon that Blix described as “one of the most toxic [nerve agents] ever developed.” Blix’s report also contained evidence that Iraq had provided contradictory information about its VX stocks in a 12,000-page declaration regarding Iraq’s weapons programs that Iraq supplied to the Security Council in December 2002. The United States and United Kingdom contended that Iraq’s false declaration to the Security Council was clear and convincing evidence of Iraq’s continued unwillingness to comply with United Nations resolutions and to peacefully disarm.

UN inspection reports provided evidence to the Security Council that Iraq had failed to account for 6,500 chemical bombs, thousand of tons of known chemical agents, empty chemical warheads (including an empty Sakr-18 chemical warhead) discovered subsequent to Iraq’s declaration, and stocks of thiodiglycol (a precursor of mustard gas).

Iraq admitted to producing—in violation of international law—8,500 liters of anthrax bacteria capable of use in biological warfare. Iraq claimed that production stopped before the first Persian Gulf War and that it destroyed the anthrax. UN inspection reports stated, “Iraq has provided little evidence for this production and no convincing evidence for its destruction.” In addition, UN inspectors concluded that there were strong indications that Iraq had manufactured far greater stores of anthrax.

Blix also reported that Iraq had manufactured a missile, the Samoud 2, that violated United Nations range restrictions limiting missiles to a range of 90 miles (150 kilometers). Inspectors also provided evidence to the Security Council that Iraq rebuilt a missile plant that had previously been destroyed by earlier inspection teams and that it continued to illegally import chemicals used in formulating missile fuels and prohibited weapons. Blix ordered Iraq to begin destruction of the prohibited missiles by March 1, 2003, and to cease production of the missiles. Blix also insisted that Iraq begin to allow U-2 reconnaissance aircraft overflights demanded by inspectors.

U.S. secretary of state Colin Powell presented additional evidence to the Security Council of Baghdad’s alleged non-compliance with UN disarmament resolutions.

Powell, accompanied to the Security Council meeting by CIA Director George Tenet, also articulated United States assertions of links between al-Qaeda and Iraq. Powell asserted Western intelligence sources had evidence that Osama bin Laden met with senior Iraqi intelligence officials and that al-Qaeda operatives enjoyed safe haven in Iraq.

Powell also contended that Iraq possessed mobile laboratories to make biological weapons. Powell played intercepts of Iraqi officers apparently ordering concealment of prohibited weapons and displayed satellite pictures of alleged chemical weapons facilities. Powell questioned Iraq’s development of unmanned drone airplanes capable of delivering chemical or biological weapons, and claimed that up to 500 tons of chemical weapons agents remained unaccounted for by Iraq.

Powell stressed that the United States and its coalition partners had “limited patience” for continued Iraqi noncompliance with United Nations resolutions. President Bush and other United States officials insisted that Iraq was in “material breach” of UN resolutions and that military action could be undertaken to disarm Iraq under the terms of existing resolutions.

Other Security Council members disagreed with U.S. and U.K. contentions and, led by France, appealed for more time to seek a peaceful resolution to the crisis. Politics—including political struggles with the European Union and NATO—intermingled with diplomacy as nations sought to position themselves with regard to a need for military action to enforce UN resolutions. France seized on the politically motivated pacifist stance of German Prime Minister Gerhard Schroder to form a unified anti-war alliance fronted by France, Germany, and Russia. Schroder, in deep political trouble regarding domestic economic problems that plagued his 2002 election campaign, ultimately secured a narrow election victory by promising socialist, Green, and anti-American elements of the German electorate that he would never allow German forces to support military action against Iraq. In addition to their anti-war stance, France, Germany, and Russia all maintained important economic interests in Iraq.

Support for France’s anti-war position reached its highest point on February 14, 2003, when French foreign minister Dominique de Villepin delivered an impassioned speech that appealed to the noblest aspirations of the United Nations. In a breach of protocol, sympathetic members applauded both de Villepin’s and the Russian foreign minister Igor Ivanov’s appeals for additional time to allow Iraq to disarm under a stricter inspections program.

The next day, February 15, 2003, saw the largest civil demonstrations for peace in the history of the world. Millions of demonstrators at sites around the globe protested potential U.S.-led military action against Iraq.

Events moved to a diplomatic breaking point in early March. France, Germany, Russia, and China staunchly opposed military enforcement of UN resolution 1441 and threatened veto of any resolution that might—even

indirectly—authorize the United States and United Kingdom to lead forces to disarm Iraq. The United States, United Kingdom, and Spain put forth a resolution that simply declared Iraq in material breach of 17 prior UN resolutions. President Bush openly declared that he would force countries to “show their cards” with regard to Iraq. In a press conference on March 6, President Bush asserted that Saddam Hussein posed a direct and immediate danger to the security of the United States and, with regard to the United Nations and pending debate and resolutions, asserted that “diplomacy has failed” and that “we really don’t need anybody’s permission” to defend the United States.

At a meeting of the Security Council the next morning, weapons inspectors Blix and El Baradei reported cooperation had improved, but that Iraqi cooperation was less than complete. Blix issued a report to the Council specifying a number of questions that remained unsolved since the passage of resolution 1441 (and previous resolutions). The UN weapons inspector’s report specifically stated that Iraq had not accounted for up to 10,000 liters of anthrax, Scud missile warheads (missiles Iraq fired at Israel and coalition forces in the Persian Gulf War and that could be armed chemical or biological agents), and drone aircraft that could fly past UN-allowed limits and that also could be fitted with spray units that could deliver chemical or biological weapons.

With war seemingly imminent, the United States, United Kingdom, and Spain amended a final resolution that set March 17, 2003, as a final deadline for the council to certify Iraqi compliance with prior resolutions. The resolution stated “...that Iraq will have failed to take the final opportunity afforded by resolution 1441 (2002) unless, on or before 17 March 2003 the council concludes that Iraq has demonstrated full, unconditional, immediate and active cooperation in accordance with its disarmament obligations under resolution 1441 (2002) and previous relevant resolutions, and is yielding possession to UNMOVIC and the IAEA of all weapons, weapon delivery and support systems and structures, prohibited by resolution 687 (1991) and all subsequent relevant resolutions, and all information regarding prior destruction of such items.”

Although a threat of force was not contained within the resolution, there was little doubt that should Iraq fail to meet the deadline, the United States and United Kingdom would lead a multinational coalition to militarily disarm Iraq. The United States also sought and promised to depose Saddam Hussein and allow the Iraqi people a chance for democratic government.

France vehemently opposed the new resolution setting specific deadlines and actively lobbied against it. The trans-Atlantic alliance between NATO allies was strained more severely than ever in its history. There were terse exchanges between diplomats and angry and severe rhetoric exchanged in the media of France and America. American press reports detailed how French intelligence officials had passed false documents to British intelligence

regarding potential Iraqi purchases of uranium. French contracts with the Iraqi dictatorship called French motives into question, and U.S. press and Western intelligence reports claimed evidence of possible sales by France to Iraq of military hardware in violation of prior UN prohibitions.

France and Russia threatened to veto the deadline resolution, and intense diplomatic efforts to sway the votes of the non-permanent members to the Security Council followed. Although the United States and United Kingdom anticipated a French veto, Prime Minister Blair promised his own government that he would seek this final resolution. With France, Russia, China, Germany, and Syria on record in opposition to the resolution, and the U.S., U.K., Spain, and Bulgaria on record in favor of the resolution, the decision rested with the remaining six temporary member states (Angola, Cameroon, Chile, Guinea, Mexico, and Pakistan). Nine votes and no veto were required to pass the resolution. Although a chance at outright passage remained slim, the U.S. and U.K. pressed for a vote before commencing military action against Iraq.

American and British diplomats claimed that the diplomatic efforts and intransigence of France ultimately “poisoned the diplomatic process.” In spite of British attempts to make amendments to pending resolutions and set specific tasks for Iraq to perform to indicate willingness to comply with UN resolutions, France promised to veto the pending resolution—in some cases before Iraq could itself reject the U.K. proposals. On March 15, President Bush, Prime Minister Blair and Spain’s President Jose Maria Anzar convened an emergency summit in the Azores where they reaffirmed the trans-Atlantic alliance and stated that March 17 would be the final date for the UN to agree on a diplomatic solution to enforce resolution 1441.

With the UN Security Council deadlocked, the probable votes of the nonpermanent members hotly disputed, and the deadline at hand, the U.S., U.K. and Spain allowed their new proposal to die without a vote. Although he had once promised to call for a vote, President Bush stated that France “had shown their cards” and administration officials declared the “diplomatic window closed.” Although France, Russia, and China declared that any U.S.- and U.K.-led coalition action against Iraq would be illegitimate and in violation of the UN charter, U.S. and U.K. officials rested on existing UN resolutions (one reason some experts claimed that another vote was not sought), Iraq’s violation of the treaty that ended the Persian Gulf War, and assertions of the right of self defense to legitimize military action.

On the evening of March 17 (Washington time), President Bush, in a televised address that was carried around the world by major news organizations, issued Saddam Hussein and his sons (both high ranking Iraqi officials) a 48-hour deadline to leave Iraq or face war.

UN weapons inspectors were withdrawn from Iraq and most countries withdrew diplomats and other personnel in anticipation of imminent war. France called for a



ministerial-level meeting of the UN Security Council, and a meeting of heads of state. The U.S. and U.K. ignored further French efforts and insisted that Hussein could only avoid war by exile.

Hussein ignored the deadline and U.S.- and U.K.-led forces launched aerial attacks against Iraq on the evening of March 19, 2002 (March 20, 2002, in Europe and Iraq).

## ■ FURTHER READING:

### PERIODICALS:

DeYoung, K., and Colum Lynch. "Britain Races To Rework Resolution: U.S. Insists on Limiting Concessions for Iraq." *Washington Post*. March 11, 2003.

Evans, D. and D. Charter. "Iraq Strikes Back with Suspected Banned Missiles." *The Times*. March 21, 2003.

Fisher, I. "Chief Weapons Inspectors See No Big Breakthrough after Talks in Baghdad." *New York Times*. February 10, 2003.

Gellman, B. "U.S. Reaps New Data on Weapons." *Washington Post*. March 20, 2003.

Sanger, D., and F. Barringer. "President Readies U.S. for Prospect of Imminent War." *New York Times*. March 7, 2003.

Tagliabue, J. "France and Russia Ready To Use Veto Against Iraq War." *New York Times*. March 6, 2003.

### ELECTRONIC:

United Nations. Security Council Resolution 1441. November 7, 2002. <<http://www.un.int/usa/sres-iraq.htm>> (March 23, 2003).

### SEE ALSO

*Iraq, Intelligence and Security Agencies*  
*Iraqi Freedom, Operation (2003 War Against Iraq)*

---

## Iraq War (Immediate Aftermath)

---

### ■ K. LEE LERNER

On May 1, 2003, United States President George W. Bush announced an end to major military combat operations related to Operation Iraqi Freedom.

Although evidence of Saddam Hussein's reign of terror was rapidly forthcoming—including the discovery of numerous mass gravesites of those brutally executed for resisting Hussein's rule—the anticipated discovery of large caches of Iraqi weapons of mass destruction (WMD)

proved elusive. By the end of May 2003, both British and American intelligence agencies began to downplay the possibility of finding large stores of such weapons. Although both U.S. and British officials continued to assert prior claims about the extent of Iraq's arsenal, questions remained as to whether the weapons had been removed, destroyed, or whether intelligence reports regarding the weapons had been mishandled, exaggerated, or falsified.

Although some seized on the growing controversy regarding the lack of WMD finds as a partisan political issue, all Western intelligence agencies, including those of war dissenter nations France and Germany, agreed before the war that Hussein's regime possessed weapons of mass destruction.

Attention in America and Europe focused on to what degree claims regarding Iraqi WMD programs might have been exaggerated, or as the British Broadcasting Corporation (BBC) reported, "sexed up" by both the Bush and Blair administrations to gain support for the war.

At the core of the controversy lay the handling of critical reports compiled by British intelligence regarding Hussein's possession and potential use of weapons of mass destruction. One report, publicly released by the British in 2002, asserted that Hussein's "military planning allows for some weapons of mass destruction to be ready within 45 minutes of an order to use them." This statement was used by Coalition governments to stress the urgency of war. Another report, also compiled by British intelligence and released just weeks before the start of military operations, allegedly had new intelligence information, but was subsequently exposed to contain material plagiarized from a previously published academic source.

A BBC report in late May 2003, alleged that a senior British official involved in the preparation of the Fall, 2002 report (containing claims regarding Iraq's ability to rapidly assemble and use biological and chemical weapons) claimed that the report was rewritten on the instructions of officials in the administration of British Prime Minister Tony Blair to make it "sexier" (i.e., to stress the urgency of war). The BBC described their source as one of a number of senior British officials in charge of drawing up the report.

Officials in the Blair government, including John Scarlett, head of the Joint Intelligence Committee, countered that the report was entirely the work product of the intelligence community and that no pressure had been exerted to change its contents. Blair administration officials demanded a retraction and apology from the BBC. The BBC refused and stood by its story. Other British government officials initially characterized the BBC sources as "rogue elements within the intelligence services" who were against the government.

The British House of Commons foreign affairs committee began a series of hearings into the controversy and took statements from government officials and journalists

regarding the BBC report. As of July 2003, the committee's initial conclusion was there was insufficient evidence of "improper influence," but that there was sufficient evidence to conclude that parts of the reports regarding Iraqi weapons readiness were given unwarranted emphasis. The committee specifically concluded that Alastair Campbell, the Blair administration's director of communications—specifically identified in BBC reports as one administration official who tried to influence report content—was not responsible for attempting to influence the contents of the report.

Another inquiry was led by the British Intelligence and Security Committee. During their hearings, testimony was provided by David Kelly, a government weapons expert. Although the BBC initially protected the identity of its source, following Kelly's death the BBC acknowledged that Kelly was the "principal source" for its claim that the report had been "sexed-up."

After the BBC aired its story in late May 2003, other news organizations sought the source of the BBC information and Kelly's name became publicly identified as the potential source of the BBC story. In July 2003, Kelly initially confirmed meeting with a BBC reporter, but denied he was the main source for the BBC report. Intense scrutiny along with and criticism of Kelly and his potential role in the story circulated in both press and government circles. Kelly blamed U.K. Ministry of Defense officials and others in the Blair government for leaking his name to the press. Kelly claimed that he was put under "intolerable" pressure by the disclosure of his association with the potential intelligence scandal.

Kelly went missing on July 17, 2003, and the next day his body was discovered near his Oxfordshire home with a knife and a packet of painkillers close to his body. Police confirmed that subsequent forensic examination concluded that Kelly committed suicide and bled to death from cuts to his wrist. Prime Minister Blair confirmed that there would be a judicial inquiry dealing with the events surrounding Kelly's death.

In July, 2003, U.S. Director of Central Intelligence, George Tenet accepted the blame for allowing subsequently discredited information from British Intelligence—that Hussein's government "recently sought significant quantities of uranium from Africa"—to remain in the text of President Bush's January 2003 State of the Union speech. Tenet acknowledged that the CIA had doubted the validity of the reports and that the evidence did not rise to the "level of certainty" normally required for insertion into presidential speeches.

At the end of July 2003, several inquiries were underway into the formulation and use by Coalition governments of intelligence related to Iraqi possession and development of weapons of mass destruction.

**The hunt for Hussein's regime.** Against steady sniper and terrorist attacks, Coalition forces continued the hunt for former officials of Saddam Hussein's regime.

In July 2003, U.S. Army soldiers and Task Force 20 personnel (a special unit tasked with capturing or killing former Iraqi leaders) surrounded and killed Qusay and Uday Hussein, Saddam Hussein's sons and top officials of the former Iraqi regime. Following their discovery in Mosul, the former Iraqi leaders refused to surrender and an intense firefight ended in their deaths. U.S. officials debated and then released photos of the bodies, in part, to alleviate Iraqi fears that the two might still be alive and attempt a return to power. U.S. officials also hoped that the confirmation of the deaths of Qusay and Uday would encourage Iraqis to come forward with intelligence related to capturing Saddam.

As of July 30, 2003, Coalition forces and Task Force 20 had killed or captured almost 40 former Iraqi leaders depicted in a famous deck of playing cards sometimes dubbed the "deck of death," circulated to Coalition forces to assist them in spotting wanted former Iraqi leaders.

At the end of July, 2003, U.S. Central Command confirmed the deaths of 90 American service personnel killed in Iraq since President Bush's May 1 declaration of an end to major combat operations. At least 49 of those soldiers were killed in combat.

## ■ FURTHER READING:

### PERIODICALS:

Schmitt, E. and B. Weinraub. "Pentagon Asserts the Main Fighting Is Finished in Iraq." *New York Times*. April 15, 2003.

Sanger D., and J. Risen. "C.I.A. Chief Takes Blame in Assertion on Iraqi uranium." *New York Times*. July 12, 2003.

### ELECTRONIC:

BBC News: "CIA Takes Blame for Iraq Claims." July 12, 2003. <<http://news.bbc.co.uk/1/hi/world/americas/3060615.stm>> (July 30, 2003).

BBC News. Timeline: "US losses in Iraq." Updated July 30, 2003. <[http://news.bbc.co.uk/2/hi/middle\\_east/3019552.stm](http://news.bbc.co.uk/2/hi/middle_east/3019552.stm)> (July 30, 2003).

United Kingdom Parliament. Oral evidence Taken before the Foreign Affairs Committee on Tuesday, July 15, 2003. <<http://www.publications.parliament.uk/pa/cm200203/cmselect/cmfaff/uc1025-i/uc102502.htm>>. July 30, 2003.

### SEE ALSO

*Iraq, Intelligence and Security Agencies*  
*Iraq War: Prelude to War (The International Debate Over the Use and Effectiveness of Weapons Inspections.)*  
*Iraqi Freedom, Operation (2003 War Against Iraq)*



A British soldier returns fire on enemy Iraqi positions to give protection to civilians fleeing the city of Basra, southern Iraq. AP/WIDE WORLD PHOTOS.

## Iraqi Freedom, Operation (2003 War Against Iraq)

■ K. LEE LERNER

After failed efforts to persuade the United Nations Security Council to endorse the use of force to disarm Iraq and oust the regime of Saddam Hussein, the United States, United Kingdom, and a coalition of countries resolved to achieve those aims through military action. Although regime change—the forced elimination of the Iraqi dictator Saddam Hussein and his sons from power—was initially only a stated goal of the United States, it became a *de facto* goal of all coalition forces.

Although Iraq's military power was not as great—and the cause not as directly apparent as the need to expel Iraqi forces following their brutal invasion and occupation of Kuwait that led to the Persian Gulf War of 1990–1991—U.S. officials asserted that Iraq's proven development and use of weapons of mass destruction in the past made Iraq a potential source of those weapons for terrorists who could then use them against U.S. or other Western targets.

In 2002, some Pentagon and administration officials urged immediate and direct action be taken by the United States to disarm Iraq. There were also more controversial calls for a regime change in Baghdad as the only means to assure Iraqi disarmament. United States President George W. Bush decided instead to seek international cooperation

to disarm Iraq. In September 2002, Bush addressed the United Nations and called for a strong resolution that, backed by the ultimate threat of the use of military force to disarm Iraq, would assure that Iraq possessed no weapons of mass destruction and assure that Iraq's capability to develop such weapons was destroyed.

In October 2002, the United States Congress voted Bush the authority to use military force to enforce UN resolutions.

In November 2002, the United Nations Security Council unanimously passed resolution 1441 that reiterated Iraq's obligations to disarm in accordance with prior treaty and resolution obligations and further recognized the threat that "Iraq's non-compliance with Council resolutions and proliferation of weapons of mass destruction and long-range missiles poses to international peace and security." Resolution 1441 proceeded to restate Security Council intentions to "restore international peace and security in the area."

U.S. secretary of state Colin Powell stressed that the United States and its coalition partners had "limited patience" for continued Iraqi noncompliance with United Nations resolutions. President Bush and other United States officials insisted that Iraq was in "material breach" of UN resolutions and that military action could be undertaken to disarm Iraq under the terms of existing resolutions.

In February and March of 2003, it became apparent that the United States, United Kingdom, and supporting countries on the United Nations Security Council could not reach a consensus with other permanent members France, Russia, and China, on the need to use immediate



On their march toward Baghdad during Operation Iraqi Freedom, U.S. Army soldiers, under fire from Iraqi troops and irregular forces guarding a key bridge over the Euphrates River at Al Hindiyah, struggle to reach an injured woman caught in the crossfire. The woman, kneeling by a civilian casualty, was ultimately rescued and carried to safety. AP/WIDE WORLD PHOTOS.

military force to enforce UN resolutions. As the diplomatic efforts stalled, war became more likely.

In late February 2003, a series of political and tactical setbacks seemingly delayed American action. Although a measure to support American bases in Turkey was supported by Turkey's president and military leaders, the Turkish parliament failed to muster a sufficient majority to pass a resolution allowing United States forces to use Turkish soil as a base for a northern front against Iraq. The resolution would have allowed Pentagon planners to place 62,000 American troops and heavy tanks along the northern Iraqi border with Turkey. It was not until after hostilities eventually started that Turkey allowed coalition forces limited use of Turkey's airspace to strike Iraq.

In the final weeks before the war, British and American air forces that had been patrolling the southern no-fly zone since the end of the Gulf War began a psychological campaign to discourage Iraqi resistance. Aircraft began dropping massive numbers of leaflets near military sites that encouraged Iraqi soldiers not to resist the overwhelming attack to come, and specifically warned Iraqi military leaders that they would be held accountable as war criminals for any use of biological or chemical weapons. In addition to radio broadcasts, psychological operations

(PSYOPS) also included targeting Iraqi officials with e-mails and phone calls designed to discourage their resistance or warn them of the consequences of war crimes.

Despite the logistical setbacks and delays, by March 5, U.S. secretary of defense Donald H. Rumsfeld and U.S. general Tommy R. Franks announced that U.S. military forces were ready to execute an attack against Iraq upon President Bush's order.

Diplomatic efforts continued to secure Turkish cooperation, but military planners set out a number of options and alternatives for war against Iraq without the immediate use of the U.S. infantry divisions and airborne forces moving southward from Turkey. One focus of the planning involved the threat of a sudden and massive first strike (termed "shock and awe" warfare) that would immediately overwhelm Iraqi defense forces. Planners worried that a gradual or escalating series of attacks would risk allowing Saddam Hussein to strike preemptively at Israel and thus potentially widen the war.

Counting army, navy, marine corps, air force and special operations forces, U.S. General Tommy Franks commanded a force of approximately 225,000 American and 25,000 British soldiers from the Central Command



A key element of the U.S.-led coalition strategy during Operation Iraqi Freedom in 2003 was the bombing of communications centers to disrupt Iraqi intelligence as well as Iraqi command and control infrastructure. Intense bombing with precision weapons destroyed the function of this Iraqi communication building without extensive damage to surrounding buildings. AP/WIDE WORLD PHOTOS.

post in Qatar. As with the Gulf War, the United States utilized a special reserve of commercial aircraft chartered specifically to transport forces to the region. An estimated 110,000 army and marine corps troops were located in Kuwait. Although the force was large, ground forces were approximately half the numbers used in the Gulf War.

Naval forces in the coalition centered upon five U.S. naval aircraft carriers located either in the Persian Gulf or eastern Mediterranean that remained within striking range of targets in Iraq. The carriers hosted air wings capable of delivering ordnance or in maintaining air superiority. In addition to the carriers, fleet forces consisted of more than two dozen missile ships and submarines—most capable of firing Tomahawk cruise missiles.

In addition to the naval air forces, more than 500 combat aircraft—including B-52s stationed in England, F117 stealth fighters, and B-2 stealth bombers—formed a powerful coalition air arsenal. For the first time in United States military history, some B-2 bombers were “forward deployed” to a base in Diego Garcia in the Indian Ocean. Special climate controlled protective hangers were constructed to maintain the sophisticated stealth capabilities of the bombers.

Without a northern front with supply bases in Turkey, U.S. tactical plans called for the launching of a massive attack from Kuwait, with the insertion of lighter forces (e.g., airborne paratroopers) into northern Iraq to secure the oil fields and other critical infrastructure in that region. Without the support of the heavy artillery of the U.S. Fourth Infantry Division, which was stalled offshore near Iraq, the lighter forces would need to take on the well-equipped and entrenched Iraqi Republican Guard units defending the northern approaches to Baghdad. U.S. leaders were also concerned that troops prevent rival Kurdish groups located in the north from starting a civil war or launching raids against Turkish forces that would further destabilize the region.

Options to open a second front without Turkish cooperation included the use of forces from the 82nd Airborne Division in Kuwait, the 173rd Airborne brigade in Italy, Army Ranger units, and elements of the 101st Airborne Division assembling in the region.

U.S. and British air strikes against Iraqi targets in the northern and southern no-fly zones increased and expanded from simple retaliation against Iraqi air defense installations that routinely fired upon U.S. and British



More than 80 percent of bombs dropped in Operation Iraqi Freedom were precision-guided ordnance. Here, smoke billows from a building in Baghdad hit by U.S.-led coalition forces during an air raid on March 31, 2003. AP/WIDE WORLD PHOTOS.

aircraft to include Iraqi ground-to-ground missile launchers (e.g., Iraqi Astros-2 rockets, a Brazilian-made multiple-rocket launcher routinely transported via truck).

Events moved to a diplomatic breaking point in early March. France, Germany, Russia, and China staunchly opposed military enforcement of UN resolution 1441 and threatened veto of any United Nations resolution that might—even indirectly—authorize the United States and United Kingdom to lead forces to disarm Iraq. The United States, United Kingdom, and Spain put forth a resolution that simply declared Iraq in material breach of 17 prior UN resolutions. President Bush openly declared that he would force countries to “show their cards” with regard to Iraq. In a press conference on March 6, President Bush asserted that Saddam Hussein posed a direct and immediate danger to the security of the United States and, with regard to the United Nations and pending debate and resolutions, asserted that “diplomacy has failed” and that the “we really don’t need anybody’s permission” to defend the United States.

With war seemingly imminent, the United States, United Kingdom, and Spain amended a final resolution that set March 17, 2003, as a final deadline for the council to certify Iraqi compliance with prior resolutions. Although a threat of force was not contained within the resolution, there was little doubt that should Iraq fail to meet the deadline, the United States and United Kingdom would lead a multinational coalition to militarily disarm Iraq. The United States also sought and promised to depose Saddam Hussein and allow the Iraqi people a chance for democratic government.

With the UN Security Council deadlocked, the probable votes of the nonpermanent members hotly disputed, and the deadline at hand, the U.S., U.K. and Spain allowed their new proposal to die without a vote. Although he had once promised to call for a vote, President Bush stated that France “had shown their cards” and administration officials declared the “diplomatic window closed.” Although France, Russia, and China declared that any U.S.- and U.K.-led coalition action against Iraq would be illegitimate and in violation of the UN charter, U.S. and U.K. officials rested on existing UN resolutions (one reason some experts claimed that another vote was not sought), Iraq’s violation of the treaty that ended the Persian Gulf War, and assertions of the right of self defense to legitimize military action.

On the evening of March 17 (Washington time) President Bush, in a televised address carried around the world by major news organizations, issued Saddam Hussein and his sons (both high ranking Iraqi officials) a 48-hour deadline to leave Iraq or face war.

Bush urged Iraqi forces not to destroy infrastructure or natural resources (e.g., oil wells), and warned Iraqi military officials that the use of chemical or biological weapons would be treated as a war crime.

After citing potential threats to American security, Bush stated, “The United States did nothing to deserve or

invite this threat, but we will do everything to defeat it. Instead of drifting along toward tragedy, we will set a course toward safety.” “The danger is clear,” Bush said. “Using chemical, biological or, one day, nuclear weapons obtained with the help of Iraq, the terrorists could fulfill their stated ambitions and kill thousands or hundreds of thousands of innocent people in our country....” President Bush also issued a message to the Iraqi people stating, “the day of your liberation is near” and promised that “the tyrant [Hussein] will soon be gone.”

Citing the increased “possibility” (indeed, some administration officials used the term “probability”) of retaliatory terrorist strikes against U.S. interests, Bush raised the terror alert level to “high” (color code orange). As of May, 2003, no such attacks occurred.

Iraq immediately denounced the ultimatum and promised defiance. UN weapons inspectors were withdrawn from Iraq and most countries withdrew diplomats and other personnel. France called for a ministerial level meeting of the UN Security Council, and a meeting of heads of state. The U.S. and U.K. ignored further French efforts and insisted that Hussein could only avoid war by exile. The British Parliament voted support of the use of U.K. forces in a military invasion of Iraq.

Sporadic fighting flared as the deadline approached. Hussein ignored the March 19 deadline, and approximately 90 minutes later—near dawn in Baghdad—U.S. jets made a strike using precision guided bunker buster bombs on a target near Baghdad believed to contain senior Iraqi officials, including Hussein. Pentagon officials subsequently said F-117 Nighthawk stealth fighter-bombers dropped 2000-pound (900-kilogram) satellite-guided bombs on a site where CIA officers developed information that Hussein might be in conference with other Iraqi leaders. For several weeks, the fate of Hussein would be debated, with Iraqi television showing images of Hussein that did not verify his survival.

Weeks later, a similar strike on an Iraqi leadership target occurred as U.S. forces were preparing to enter Baghdad. Once again, the fate of Hussein and other leaders remained uncertain.

Coalition intelligence services and special operations units played an important role in identifying and in some cases physically “painting” targets. Target painting refers to the process of identifying a target with a laser or an electronic signature device that allows weapons platforms (e.g. airplanes, tanks, etc.) to identify targets. Coalition special forces and intelligence units—including CIA units—operated inside Iraq for weeks prior to the initial attack. In addition to identifying targets, intelligence and psychological operations (PSYOPS) teams dropped tens of thousands of leaflets, and made radio broadcasts designed to discourage Iraqi resistance and possibly spark a coup against Hussein. Special efforts were made to psychologically separate regular Iraqi units, better trained Iraqi Republican Guard units, and Hussein’s inner circle to facilitate the surrender of as many Iraqi forces as possible.

Bush made a further television address to announce the start of hostilities. Across Iraq, U.S. forces launched probing attacks, along with attacks to destroy Iraqi command and control facilities. Anti-aircraft radar and missile facilities were the targets of Tomahawk cruise missiles launched by U.S. naval vessels, and U.S. aircraft dropped precision-guided bombs against targets.

Hours after the U.S. strikes, Iraq fired at least four missiles into northern Kuwait. According to American officials, Patriot missiles intercepted at least two missiles. Fear of chemical attacks by Iraq forced coalition forces and residents of northern Kuwait to repeatedly put on protective clothing and gas masks. Subsequent analysis of missile remains—and others eventually launched into Kuwait—indicated that the missiles carried conventional, not chemical, warheads.

Fear of the use of weapons of mass destruction was based upon Hussein's use of chemical weapons against Iranian forces during the 1980s Iran-Iraq War, and his prior use of chemical weapons against civilians in rebellious areas of Iraq.

In an attempt to prove that Hussein had survived the initial attack and thus forestall possible Iraqi defections, Iraqi television broadcast a speech allegedly by Hussein. Western intelligence sources could not immediately verify that the speech was actually made by Hussein. Intelligence officials had long known that Hussein had a number of body doubles—some surgically altered to bear a closer resemblance to the Iraqi leader.

On March 20, U.S.-led forces intensified attacks and forces breached Iraqi defensive positions and barriers along the Kuwait border. Tank and mechanized infantry units penetrated nearly 100 miles (160km) into Iraq by the end of the first day. Embedded journalists relayed back video of tank units racing across the Iraqi desert toward Baghdad. British forces raced to surround and isolate the port city of Basra. U.S. forces began the mechanized march to Baghdad.

A brief lull in the aerial attacks on Baghdad by coalition forces, along with statements by U.S. officials regarding the potential surrender of significant portions of Iraq's Republican Guard units, provided additional evidence of special forces and intelligence unit contact with Hussein's inner circle. The lull in attacks against Baghdad also fueled speculation about whether Hussein was still alive, or in complete control of his forces.

In a Pentagon press briefing, Rumsfeld said, "We are in communication with still more people who are officials of the military at various levels, the regular army, the Republican Guard, the Special Republican Guard...." Offering surrender, Rumsfeld added, "We continue to feel that there's no need for a broader conflict if the Iraqi leaders act to save themselves and to prevent such further conflict." Although there were significant defections and surrenders of Iraqi forces, nothing approached the mass surrenders anticipated by optimistic U.S. officials.

On March 21, U.S.-led coalition forces launched a massive aerial bombardment of Baghdad and other targets throughout Iraq. GPS precision guided bombs and an estimated 300 cruise missiles targeted Iraqi command and control facilities. Within an hour of the start of the attack on Baghdad, coalition forces destroyed more than 25 major buildings that housed Iraqi governmental offices. Hussein's presidential palaces in and around Baghdad were also destroyed.

The March 21 assault, designated by Pentagon planners as "A-Day" (aerial attack day), was the start of the "shock and awe" pattern of precise, but massive attacks designed to stun the Iraqis into submission.

At a Pentagon press briefing Rumsfeld made a special effort to address comparisons of the coalition "A-Day" attacks to similar massive attacks during WWII (e.g. the firebombing of Dresden). Rumsfeld dismissed the comparisons as invalid because of the use of precision weapons against military and government targets as opposed to the deliberate use of "dumb bombs against broad areas."

Over the next three weeks, coalition forces moved farther and faster than any army in history. British forces surrounded Basra and Umm Qasr, and systematically took control of the cities with minimal losses. Within days the entire coastline of Iraq was under coalition control, although terrorist actions and pockets of resistance worked to slow the promised quick delivery of humanitarian assistance to Iraqis falling under U.S. control.

Special forces helped secure airfields designated H2 and H3 in the western region of Iraq. These forces also help control the "Scud box" area from which Iraq had launched missiles against Israel during the Gulf War.

On the road to Baghdad, U.S. troops fought battles in Najaf, Kut, and waged a pitched battle in Nasiriya before capturing a key bridge over the Euphrates River. U.S. forces fought Iraqi troops, terrorist guerrillas known as Martyrs of Saddam who engaged in suicide bombings, and fedayeen militia conducting suicide attacks. This was often complicated by Iraqi use of civilian human shields. However, the biggest delays in the U.S. advance were caused by a major sandstorm that precluded helicopter operations and the need to secure rapidly extending supply lines from rearward attacks by troops and guerilla forces bypassed on the lightening thrust toward the Iraqi capital. U.S. forces also encountered fierce fighting in Karbala.

Coalition forces were also slowed by the need to wear clothing and equipment designed to protect them against chemical or biological weapons, although such protection ultimately proved unnecessary.

For a few days, American forces conducted operations about 100 miles south of Baghdad before resuming their push toward the city.

The war was the most intensely covered news event in history. Journalists embedded with coalition forces provided live pictures from the battlefield. In terms of both quantity and quality of coverage, the war was a profound



event in media history. In many cases, the same facts were reported with vastly differing emphasis depending on the reporter's perspective or political/editorial orientation of the news agency. At other times, there were wide discrepancies in the amount of airtime or print space offered to particular stories. For the first time, several Arab television news channels, including Al-Jazeera, provided continuous coverage that competed with U.S.-based news organizations, the BBC, and European based news organizations.

While coalition forces were lauded by reporters and commentators from some news organizations for the use of precision weapons that reduced civilian casualties, other organizations continually emphasized graphic pictures of civilian and military casualties. Al-Jazeera, criticized before the war by many Western media editors for airing biased, inaccurate, and inflammatory anti-Western reports, drew intense criticism from U.S. officials for showing controversial video of coalition POWs held or executed by Iraqis.

Although considered an almost comical media side-show by Western news agencies, the farcical interviews and briefings conducted by Iraq's minister of information, Said Sahaf, were reported more seriously by Arab news channels. Even as U.S. troops raced toward Baghdad, Sahaf continued to insist that U.S. troops had been "slaughtered," and "driven out of the country." When U.S. troops were literally within blocks of his Baghdad location, Sahaf confidently told reporters that American troops were not within 100 miles of Baghdad. Belief in Sahaf's assurances and boasts about the power of the Iraqi army (once the third largest ground force in the world) engendered shock and surprise among some viewers of Al-Jazeera and other Arab news outlets when the Iraqi government abruptly collapsed soon afterward.

Although coalition forces ultimately managed a quick and decisive military victory, the effects of the differing perspectives in news coverage may take years to fully determine.

Given the demanding pace of round-the-clock media coverage, operational pauses for rest or logistical resupply by coalition forces often led to open speculation as to whether coalition forces were "bogged down." Delays caused by duststorms, and deaths caused by suicide bombers attacking checkpoints caused some commentators to openly speculate that America was getting involved in "another Vietnam-like quagmire" or that the war could stretch on for many months, perhaps years.

The use of fewer troops than used in the Gulf War also drew criticism. The war plan was a test of a new policy of smaller force deployments. Advocates of the lighter force concept argued that mobility, precision weapons, and real-time integration of intelligence information acted as "force multipliers." Pentagon or war plan critics contended that the U.S. had not deployed adequate ground troops to ensure maximum safety for both military personnel and Iraqi civilian populations.

Despite criticisms, within three weeks, coalition forces toppled the Hussein regime. The speed of attack also allowed coalition forces to accomplish major goals. Iraqi command and control was virtually eliminated within hours of the start of military operations. The Iraqis could offer little organized resistance. U.S., British, and Australian forces secured both southern, and then northern, oil fields before Hussein's forces could set significant fires or cause significant environmental damage as they did during the Gulf war. The Iraqi air force was totally destroyed or immobilized and launched no sorties against coalition forces. In the north, a major terrorist facility was overrun and destroyed.

In a battle on April 2, army and marine troops routed the elite Iraqi Republican Guard units about 20 miles of south of Baghdad and a two-pronged assault on the capital began. On April 4, U.S. troops seized Baghdad's main airport located just 10 miles from the center of the city.

After brief preliminary incursions, on April 9, U.S. forces advanced into central Baghdad and Saddam Hussein's government was symbolically toppled. Carried live by global television networks, Iraqis celebrating liberation—with the technical assistance of U.S. troops—pulled down a large statue of Saddam Hussein located in central Baghdad. Kurdish fighters and U.S. forces secured the northern cities of Kirkuk and Mosul during the next three days.

On April 15, U.S. marines captured Tikrit, the ancestral home of Saddam Hussein. After an intense bombardment, U.S. forces encountered only sporadic resistance as they captured what was thought to be Hussein's last military stronghold. Pentagon officials stated that the main military fight in Iraq was finished.

The speed of the American advance and coalition determination not to be seen as oppressive occupying powers unfortunately resulted in a lack of policing activities and resultant looting. Iraqi looters and criminals from other countries stole freely and openly, in some cases taking valuable artifacts and cultural treasures. The looting, and perceived slowness in restoration of water and electricity, sparked anti-American protests in newly liberated Iraq. Religious fundamentalists also took the opportunity afforded by liberation to begin to organize anti-Western protests.

Nine weeks after the start of military action against Iraq, the United Nations Security Council—including France, Russia, and China—overwhelmingly approved a resolution lifting economic sanctions against Iraq and gave its backing to U.S.-led administration by coalition forces until the situation in Iraq stabilized.

The lack of success in finding massive stockpiles of biological or chemical weapons spurred charges that the CIA and other Western intelligence agencies had exaggerated reports of Iraqi capabilities in this area. Even the French government, one of the harshest critics of U.S. war plans, had openly accepted that large stockpiles of chemical and biological agents existed in Iraq prior to the war.

Although French intelligence reports disagreed with American and British assessments of ongoing links between Iraq and al-Qaeda, French Foreign Minister Dominique de Villepin stated that his sources nevertheless confirmed much of the information regarding biological and chemical weapons stockpiles reported by U.S. and U.K. intelligence services. De Villepin, however, dismissed CIA and MI-6 information as common knowledge among Western intelligence services and therefore not a cause for immediate war.

As of May 2003, coalition teams were continuing to explore for sites containing weapons of mass destruction. Although there were many preliminary findings of illegal equipment that might have been used to manufacture such weapons, none had yet withstood careful scientific scrutiny. U.S. officials invited international inspectors to examine specific finds (e.g., suspected mobile biological weapons laboratories.)

UN chief weapons inspector Hans Blix subsequently concluded that Iraq may not have had weapons of mass destruction—or at least not on the scale previously anticipated, and that Saddam Hussein’s evasive behavior with inspectors may have resulted from his dictatorial need to control information. U.S. officials openly speculated about the possible diversion of weapons to Syria and accused Syria of harboring deposed Iraqi leaders and of attempting to develop and test chemical weapons. Syria denied the U.S. allegations.

Leading administration officials claimed that inspection efforts would take many months and that the best hope of finding weapons stockpiles would come from the interrogation of captured Iraqi leaders and scientists. Intelligence reports leaked to the press also indicated that there was evidence of massive smuggling of materials (including possible weapons shipments) into Syria. There was also mounting evidence that during the diplomatic infighting prior to the war the French and Russian governments had provided assistance to Iraqi leaders as they attempted to conceal the extent of their support of the Hussein regime. British press reporters discovered documents with Bin Laden’s name covered with correction fluid that, if ultimately proved genuine, would provide evidence of formal communications and cooperation between the Hussein regime and al-Qaeda.

Unarguable evidence concerning the brutality of Hussein’s regime was provided with the discovery of mass gravesites at Abul Kasib, Basra, Najaf, al-Mahawil, Babylon, Muhammad Sakran, and Kirkuk. Many of the graves contained men, women, and children apparently executed after failed uprisings against Saddam Hussein. South of Baghdad, many graves contained those executed following the attempted Shia rebellion that followed the Gulf War. Northern mass graves contained the remains of political prisoners and Kurds executed during Hussein’s policy of ethnic cleansing.

As of May 2003 the whereabouts or fate of Hussein and other top Iraqi leaders remained uncertain. The U.S.

abolished the Baath Party and security institutions of Saddam Hussein’s former regime. With Iraq occupied and administered by coalition forces, the U.S. removed Iraq from the list of countries not cooperating with the fight against terrorism.

Coalition goals and plans for the postwar stabilization of Iraq asserted that coalition forces would maintain physical civil security, while U.S.-administered government departments regulate infrastructure and aid. Under Coalition guidance, Iraqi citizens and returning expatriates would be encouraged to form a broad-based, multi-ethnic interim Iraqi administration that would eventually become a self-governing Iraqi government recognized by the international community.

#### ■ FURTHER READING:

##### PERIODICALS:

Gordon, M. “The Test for Rumsfeld: Will Strategy Work?” *New York Times*. April 1, 2003.

Sanger, D., and F. Barringer. “President Readies U.S. for Prospect of Imminent War.” *New York Times*. March 7, 2003.

Schmitt, E., and T. Shanker. “U.S. Reports Talks Urging Surrender of Elite Troops.” *New York Times*. March 21, 2003.

Schmitt, E. and B. Weintraub. “Pentagon Asserts the Main Fighting Is Finished in Iraq.” *New York Times*. April 15, 2003.

Tyler, Patrick E. “Hussein Statue Is Toppled—Rumsfeld Urges Caution.” *New York Times*. April 10, 2003.

##### ELECTRONIC:

BBC News. Iraq War. Key Maps. <[http://news.bbc.co.uk/1/shared/spl/hi/middle\\_east/03/v3\\_iraq\\_key\\_maps/html/graves/link1.stm](http://news.bbc.co.uk/1/shared/spl/hi/middle_east/03/v3_iraq_key_maps/html/graves/link1.stm)> (May 12, 2003).

Central Intelligence Agency. “Iraq.” *CIA World Factbook* <<http://www.cia.gov/cia/publications/factbook/geos/iz.html>> (May 25, 2003).

U.S. Department of Defense. Operation Iraqi Freedom Special Report. “President Bush Outlines Progress in Operation Iraqi Freedom.” <<http://www.whitehouse.gov/news/releases/2003/04/iraq/20030416-9.html>> (April 16, 2003).

##### SEE ALSO

*International Atomic Energy Agency (IAEA) Iraq, Intelligence and Security Agencies in Iraq War: Prelude to War (The International Debate Over the Use and Effectiveness of Weapons Inspections.)*

---

## Ireland, Intelligence and Security

---

The failed Easter Rebellion of 1916 sparked decades of guerilla warfare and terrorist attacks in Ireland. Ireland

finally gained its independence from Britain in 1921, but the accord that granted the establishment of the Irish Republic also divided the island. Six northern counties, now Northern Ireland, remained in British possession. The partitioning of Ireland brought relative peace to the Irish Republic, but initiated decades of violent conflict between Irish loyalists and British unionists in the north. After remaining officially neutral during World War II, Ireland withdrew from the British Commonwealth in 1948 in protest over continued English rule in Northern Ireland.

Despite earlier conflict, Ireland and Britain have worked closely to stem terrorism and political conflict in Northern Ireland and throughout the British Isles. Today, Ireland is enjoying relative calm in the Northern Ireland conflict. A series of peace accords and disarmament treaties between rival factions in the region have yielded limited successes. In 2001, Irish intelligence and security forces joined a European coalition to fight global terrorism. While not a member of the North Atlantic Treaty Organization (NATO), the Irish republic is an influential member of the European Union.

Ireland maintains a stated policy of neutrality, however the nation has a sizable military. The *Óglaigh na h-Éireann*, or Irish Defense Forces, have two dedicated intelligence and security divisions. The G-2 military intelligence branch collects and analyzes both foreign and domestic intelligence. The agency often aids other European nations and the United States in international intelligence operations. G-2 provides intelligence information on terrorist organizations associated with the Northern Ireland conflict, often cooperating with British intelligence at MI5. G-2 is one of Europe's most sophisticated intelligence agencies, conducting remote, computer systems, signals, and human surveillance.

The Irish Defense Forces also possess a highly specialized action unit known as the *Sciathán Fianóglach an Airm*, or Army Ranger Wing. Recognizing the need for a special deployment force to respond to terrorist threats and hostage situations, the Irish government arranged for the training of an elite force of Irish Defense soldiers at the United States Army Ranger School at Ft. Benning, Georgia. The specially trained unit returned to Ireland to train other military personnel. In 1980, the official Army Ranger Wing was formed. The Army Rangers conduct counterterrorism operations, and are trained in hostage rescue and urban street fighting.

In addition to military forces, Ireland's largest civilian security force is the *An Garda Síochána*, known commonly as the Garda. The Garda is the Republic of Ireland's national police force. The main charge of the agency is the protection of citizens and domestic national interests. In conjunction with the Army Ranger Wing, the security and intelligence unit of the Garda conducts regular counterintelligence surveillance. The Special Branch C3 Section is the Garda's elite counterterrorism unit.

Ireland is one of Europe's leading sites of technological and computer systems. The growth of Ireland's technology industry has increased the need for corporate and economic security. The Garda and other Irish government agencies have increased efforts to thwart corporate espionage, money laundering, and the illegal trafficking of technology and funds to suspected terrorist organizations.

While terrorism related to the conflict in Northern Ireland has substantially subsided in recent years, the Irish intelligence community continues extensive counterterrorism operations. Irish Defense Forces have trained counterterrorism forces from other European nations. In response to increasing global terrorism threats, the Irish Defense Forces and Garda are preparing heightened defense structures and tightening domestic security measures in preparation for the Irish Presidency of the European Union in 2004.

#### SEE ALSO

*European Union*  
*United Kingdom, Counter-terrorism Policy*

---

## Irish Republican Army (IRA)

---

The Irish Republican Army (IRA) also operates as, or is known as, the Provisional Irish Republican Army (PIRA or "Provos").

The IRA formally became a terrorist group in 1969 as the clandestine armed wing of Sinn Féin, a legal political movement dedicated to removing British forces from Northern Ireland and unifying Ireland. The IRA originated with a Marxist orientation and was organized into small, tightly knit cells under the leadership of the Army Council. The IRA has been observing a cease-fire since 1997 and in October 2001, took the historic step of putting an unspecified amount of arms and ammunition "completely beyond use." The International Commission on Decommissioning characterized the step as a significant act of decommissioning. The IRA retains the ability to conduct operations. Its traditional activities have included bombings, assassinations, kidnappings, punishment beatings, extortion, smuggling, and robberies. Bombing campaigns were conducted against train and subway stations and shopping areas on mainland Britain. Targets included senior British government officials, civilians, police, and British military targets in Northern Ireland.

The IRA has, at a minimum, several hundred members, plus several thousand sympathizers—despite the possible defection of some members to the Real IRA (RIRA). The IRA operates in Northern Ireland, the Republic of Ireland, Great Britain, and Europe. During its history,

the IRA has received aid from a variety of groups and countries and considerable training and arms from Libya and the Palestinian Liberation Organization. The IRA is suspected of receiving funds, arms, and other terrorist related materiel from sympathizers in the United States.

#### ■ FURTHER READING:

##### ELECTRONIC:

CDI (Center for Defense Information) Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <<http://www.cdi.org/terrorism/terrorist.cfm>> (April 17, 2003).

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001." Annual Report: On the Record Briefing. May 21, 2002 <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

##### SEE ALSO

*Terrorism, Philosophical and Ideological Origins Terrorist and Para-State Organizations Terrorist Organization List, United States Terrorist Organizations, Freezing of Assets*

## Islamic Army of Aden (IAA)

Islamic Army of Aden (IAA) also operates as, or is known as, the Aden-Abyan Islamic Army (AAIA).

The IAA emerged publicly in mid-1998 when the group released a series of communiqués that expressed support for Osama Bin Laden (also spelled Usama Bin Ladin) appealed for the overthrow of the Yemeni government and the commencement of operations against U.S. and other Western interests in Yemen. The IAA engages in bombings and kidnappings to promote its goals. IAA members kidnapped 16 British, Australian, and U.S. tourists in late December 1998 near Mudiyah in southern Yemen. Since the capture and trial of the Mudiyah kidnapers and the execution in October 1999 of the group's leader, Zein al-Abidine al-Mihdar (a.k.a. Abu Hassan), individuals associated with the IAA have remained involved in terrorist activities. In 2001, the Yemeni government convicted an IAA member and three associates for their roles in the October 2000 bombing of the British Embassy.

IAA operates in the southern governorates of Yemen—primarily Aden and Abyan.

#### ■ FURTHER READING:

##### ELECTRONIC:

CDI (Center for Defense Information) Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <<http://www.cdi.org/terrorism/terrorist.cfm>> (April 17, 2003).

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001." Annual Report: On the Record Briefing. May 21, 2002. <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

##### SEE ALSO

*Terrorism, Philosophical and Ideological Origins Terrorist and Para-State Organizations Terrorist Organization List, United States Terrorist Organizations, Freezing of Assets*

## Islamic Movement of Uzbekistan (IMU)

Islamic Movement of Uzbekistan (IMU) is a coalition of Islamic militants from Uzbekistan and other Central Asian states opposed to Uzbekistani President Islom Karimov's secular regime. Before the counterterrorism coalition began operations in Afghanistan in October 2001, the IMU's primary goal was the establishment of an Islamic state in Uzbekistan. If IMU political and ideological leader Tohir Yoldashev survives the counterterrorism campaign and can regroup the organization, however, he might widen the IMU's targets to include all those he perceives as fighting Islam. The group's propaganda has always included anti-Western and anti-Israeli rhetoric.

**Organization activities.** The IMU primarily targeted Uzbekistani interests before October 2001 and is believed to have been responsible for five car bombs in Tashkent in February 1999. IMU militants also took foreigners hostage in 1999 and 2000, including four U.S. citizens who were mountain climbing in August 2000, and four Japanese geologists and eight Kyrgyzstani soldiers in August 1999. Since October 2001, the coalition has captured, killed, and dispersed many of the militants who remained in Afghanistan to fight with the Taliban and al-Qaida, severely degrading the IMU's ability to attack Uzbekistani or coalition interests in the near term. IMU military leader Juma Namangani apparently was killed during an air strike. As of May 2002, Yoldashev remained at large.

Islamic Movement of Uzbekistan militants probably number under 2000 and are scattered throughout South Asia and Tajikistan. Areas of operations for the IMU include Afghanistan, Iran, Kyrgyzstan, Pakistan, Tajikistan, and Uzbekistan. Receiving support from other Islamic extremist groups and patrons in the Middle East and Central and South Asia, the IMU leadership also broadcasts statements over Iranian radio.

## ■ FURTHER READING :

### ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001. Annual Report: On the Record Briefing. May 21, 2002. <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

### SEE ALSO

*Terrorism, Philosophical and Ideological Origins*  
*Terrorist and Para-State Organizations*  
*Terrorist Organization List, United States*  
*Terrorist Organizations, Freezing of Assets*

---

## Isotopic Analysis

---

### ■ ALEXANDR IOFFE

Varieties of the same chemical element, but with different atomic weights, are called isotopes. Isotopic analysis (IA) is the analysis of the isotope composition of a sample. Samples in IA can contain almost anything: different objects of everyday life, pieces of rocks, pieces of wood, samples of tissue taken from a human body, chemical compounds, and so on. In general, and with some degree of simplification, isotopic analysis is used for identification of a sample and for the determination of its age. Isotopic analysis is based upon the use of mass spectrometers or radioactive radiation counters. A mass spectrometer is a device that determines the quantity and composition of different isotopes (of the same chemical element as well as various elements) in the sample.

The Oak Ridge National Laboratory in 2001 designed a portable mass spectrometer that is capable of detecting chemical and biological agents of war in the air, and can also detect chemical warfare agents on the ground. Called the chemical-biological mass spectrometer (CBMS), the device works by collecting an air sample or chemical sample via a chemical probe and classifying it first according to its size, then according to its unique ion products. The system can detect a wide range of chemical and

biological weapons on the battlefield, such as anthrax spores, nerve gas, viruses, and toxins. The CMBS is scheduled to be manufactured in sufficient numbers to be operational in the field by 2004.

Another new mass spectrometry device, similar to the walk-through scanners used in airports, may soon be able to detect microscopic amounts of explosives or narcotic substances hidden in clothing or on a person. When passing through the scanner, a jet of air puffs clothing and air samples immediately surrounding the person are concentrated and analyzed using ion mobility spectrometry. Minute amounts of explosives, chemical weapons, and illegal drugs that cling to the skin or clothing can be easily found. The highly sensitive nature of the scanner can also be a drawback, as targeted substances may be found on persons unaware of their presence. For example, the scanner could detect a narcotic residue on coins randomly received at an airport vending machine by an unsuspecting person. The likelihood for false positive results, along with the high cost of the machine and the seven-second period necessary to scan each individual, may inhibit its widespread use in airports. Some airports do use similar technology to screen checked baggage.

The isotope composition of many objects is unique (relative to the composition itself as well as to the isotope concentrations), and because of this, isotopic analysis offers the possibility for identification of a sample. Isotopic analysis is also utilized in varying disciplines, including chemistry, medicine, biology, geology, archeology, and criminal forensics. Recently, isotopic analysis has seen use in the diagnosis of some diseases through analysis of air exhaled by the patient. Often, isotopic analysis permits the scientist to distinguish the genuine product from its imitation. For example, the technology is used to distinguish expensive types of wine and liquor from their imitations. When archaeologists investigate various fragments of ancient objects, they sometimes use isotopic analysis to determine where these objects were made, or to elucidate the source of the raw material for their production.

Isotopes can be both stable and radioactive. Isotopic analysis of radioactive isotopes permits scientists to determine the age of the investigated sample. Often the isotope  $C^{14}$  is used for this purpose. This isotope itself is unstable and decays with time, and in the decay process, other stable isotopes are created. In nature, the concentration of  $C^{14}$  is maintained because of cosmic radiation. While a tree lives, for example, the concentration of  $C^{14}$  in its wood is equal to the  $C^{14}$  concentration in the environment, because atoms of radioactive carbon penetrate the wood from the atmosphere with  $CO_2$  molecules due to photosynthesis, and also through the tree root system. But when the tree dies, these exchange processes cease, and the  $C^{14}$  concentration in the tree begins to decrease. The law of radioactive carbon concentration alteration in the sample is known, hence if its concentration is measured in the sample and compared with the concentration of the isotope in nature, the age of the tree itself can be

determined (or more precisely, the time since the tree died). When the decay period of the radioisotope is considered, the age of the sample can be determined within an accuracy of several decades. For this analysis, a sample weight of only several milligrams (mg) is often sufficient. For example, a mammoth calf whose body was recently found in Siberia in the frozen ground was determined to have lived about 27,000 years ago, and only 4 mg of the mammoth muscle tissue was needed for the analysis.

## ■ FURTHER READING :

### ELECTRONIC:

Lawrence Livermore National Laboratory. "National Resource for Biomedical Accelerator Mass Spectrometry." <<http://www.llnl.gov/bioams/index.html>> (January, 4, 2003).

"New Airport Security Measures." l-mass.com. <<http://l-mass.com/airp1100.html>> (January, 4, 2003).

Oak Ridge National Laboratory. "Chemical Biological Mass Spectrometer." <<http://infosrv1.ctd.ornl.gov/ORNLRview/measure/analy/direct/chem-bio.htm>> (January, 4, 2003).

### SEE ALSO

*Air Plume and Chemical Analysis*

*Biological Warfare*

*Gas Chromatograph-Mass Spectrometer*

*Microbiology: Applications to Espionage, Intelligence, and Security*

## Israel, Counter-Terrorism Policy

■ TIMOTHY G. BORDEN

Since it was founded in 1948, the nation of Israel has implemented some of the most rigorous counter-terrorist measures of any country in the world. It suffered its first attacks by the Palestine Liberation Organization (PLO) in 1965 and was subject to PLO Intifadas, or uprisings, in 1987 and again in 2001, which produced dozens of terrorist bombings with hundred of casualties. Israel's zeal to contain and prevent terrorist attacks against its citizens has at times prompted international criticism, particularly regarding its state-sponsored assassinations of known terrorists in other countries and use of coercive interrogation to gather information on terrorist activities.

Israel has perhaps the greatest experience with counter-terrorist measures than any other modern nation. Facing hostility from its Arab neighbors, the Jewish state enacted the Prevention of Terrorism Ordinance upon its

establishment in 1948. The law defined terrorism to include direct acts of violence as well as threats of violence against an individual, and broadly categorized membership in a terrorist organization to include those who had given money or resources to such a group in addition to those who directly participated in it. The 1948 ordinance also gave authorities such as Shin Bet, the country's intelligence agency, broad prosecutorial powers to detain individuals and shut down suspected terrorist centers. Later amendments to the 1948 ordinance made it illegal to sympathize with terrorist organizations by flying their flags or displaying their symbols and criminalized most contacts made abroad with terrorists (a stipulation repealed in 1993).

Although Israel's counter-terrorist policies were sometimes criticized as being too harsh, its citizens came to expect a high degree of government vigilance over their daily lives. Much of the counter-terrorist effort was resource-intensive, not technologically sophisticated. Searches of individuals and their belongings were routine in public places, and scrutiny at border crossings and the country's main international airport was intense. The government rigorously screened all employees manning security checkpoints at airports and borders and travelers at borders were asked extensively about their travel plans, sources of income, contacts in Israel, and other personal issues.

Although the scrutiny with which Israel conducted such inquiries provoked accusations of anti-Arabic racial profiling, it was largely responsible for producing a near-perfect record of safety on the government-owned airline, El Al. The only incident of hijacking on El Al occurred in July 1968, when three members of the Popular Front for the Liberation of Palestine took control of a plane on its way from Rome to Tel Aviv. The hijackers held the plane's passengers hostage for forty days until Israel acceded to their demands for the release of a group of Palestinian terrorists.

The Israeli government stiffened its resolve to follow a zero-tolerance policy in negotiating with terrorists in June 1976, when a group of Palestinian and German terrorists abducted an Air France plane and held its passengers hostage at an airport in Entebbe, Uganda. After the hijackers demanded the release of fifty-three jailed Palestinian terrorists during an eight-day standoff, an Israeli commando squad stormed the plane and ended the siege. All of the hijackers were killed in the raid. The lives of 98 hostages were saved; four hostages were killed in the raid.

Despite the continuing emphasis on counter-terrorism in Israel, an Intifada, or uprising, sponsored by the PLO from 1987 onward against the Israeli presence in the Occupied Territories resulted in at least 20,000 casualties on both sides. Although tensions subsided after the withdrawal of Israeli troops from much of the Occupied Territories under a series of accords from 1993 to 1997, Israeli citizens continued to face terrorist threats on a daily basis.

In 2001, a renewed wave of Intifada actions resulted in dozens of bombings on Israeli soil, which occurred at the rate of two every month. Given the ongoing threat, about 10 percent of the Israeli gross national product is annually spent on defense.

## ■ FURTHER READING:

### BOOKS:

Heller, Mark A. *Continuity and Change in Israeli Security Policy*. New York: Oxford University Press, 2000.

Inbar, Efraim. *Rabin and Israel's National Security*. Baltimore: Johns Hopkins University Press, 1999.

James, Ron. *Frontiers and Ghettos: State Violence in Serbia and Israel*. Berkeley: University of California Press, 2003.

Katz, Samuel M. *The Hunt for the Engineer: How Israeli Agents Tracked the Hamas Master Bomber*. New York: Fromm International, 1999.

Thomas, Gordon. *Gideon's Spies: The Secret History of the Mossad*. New York: St. Martin's Press, 2000.

### PERIODICALS:

Gladwell, Martin. "Safety in the Skies." *New Yorker*. October 1, 2002.

Morris, Jim. "Israel Offers Lessons in Aviation Security." *Dallas Morning News*. November 8, 2001.

Schwartz, Nelson. "Learning from Israel." *Fortune*. (January 21, 2002).

### SEE ALSO

*Airline Security*

*Egypt, Intelligence and Security*

*Eichmann, Adolf: Israeli capture*

*Intelligence and Democracy: Issues and Conflicts Mossad*

*Palestinian Authority, Intelligence and Security*

*Pollard Espionage Case*

*Syria, Intelligence and Security*

*Terrorism, Philosophical and Ideological Origins*

*Terrorist and Para-State Organizations*

Israel in the south, and Arab Palestine in the north. To ease hostility between the two factions, the city of Jerusalem, holy to Jews, Muslims, and Christians, was declared an international city. A series of wars between Israel and its Arab neighbors led to an expansion of Israeli territory, including gaining control of Jerusalem, and heightened animosity between Jews and Arabs in the region.

## The Israeli Intelligence Community

Israel built its intelligence and security communities to ensure the survival of the precarious state. Israel's first intelligence forces were groups of special agents whose task was to locate Nazi war criminals and either assassinate them, or bring them to justice. The government then trained agents to spy on rival governments and militaries in the Middle East. By the 1960s, the Israeli intelligence service was one of the most well-trained, sophisticated, and effective intelligence services in the world.

Today, four primary agencies comprise the Israeli intelligence community. Israeli intelligence services are divided along traditional lines, but all Israeli intelligence officers receive military training due to the nation's policy of compulsory service.

**The Center for Political Research.** The Ministry of Foreign Affairs creates and implements Israel's foreign policy. The ministry supports and oversees the Center for Political Research, which monitors the political climate of the Middle East. The Center's mission is to collect and analyze information about political organizations, public political attitudes, and rival governments. Research analysts use openly available sources, as well as intelligence information, to advise the Minister of Foreign Affairs and the Office of the Prime Minister. The Center for Political Research also aids Israeli missions overseas, and advises allied foreign intelligence services on Middle East issues.

**Mossad.** The Institute for Intelligence and Special Tasks, more commonly known as the Mossad, is Israel's primary intelligence agency. Mossad is responsible for human intelligence and covert actions. Formed in 1951 to hunt for fugitive Nazi war criminals, the agency began as a collection of special forces units. To a lesser extent, Mossad maintains that organizational tradition today, and contains several small forces tasked with specific responsibilities and covert operations. Mossad task force agents assist with the movement of Jewish refugees out of hostile territories, attempt to infiltrate and sabotage Palestinian nationalist groups, and conduct counterintelligence operations.

In addition to numerous specialized forces, the Mossad maintains eight operational divisions. The Collections Department, Mossad's largest, administers Israel's extensive human intelligence network. The department focuses

# Israel, Intelligence and Security

Israel gained its independence following World War II after Britain ended its colonial mandate of Palestine. Jewish refugees and victims of the Holocaust immigrated to Palestine in order to create the Jewish homeland promised in the British Balfour Declaration. The influx of immigrants created tension in the Arab dominated region. The United Nations intervened, creating the Jewish state of



Israeli nuclear spy Moredechai Vanunu, right, sits next to his lawyer during his trial in Beer Sheva in 1998 for revealing Israel's secrets. AP/WIDE WORLD PHOTOS.

on foreign intelligence operations, conducting espionage under a variety of diplomatic and industrial covers.

The Political Action and Liaison Department coordinates Mossad activities and shares information with allied nations. These agents are usually stationed in Israel's foreign embassies.

Mossad's third largest division, the Research Department, processes all intelligence material collected by Mossad field agents. Researchers also produce detailed reports, using openly available sources, for use by Mossad agents, the military, and other government agencies. The Research Department is subdivided into fifteen desks, each overseeing information regarding a specific geographic location. A specially dedicated desk monitors nuclear issues, such as weapons proliferation and development.

Mossad employs propaganda and deception operations with the aid of the Lohamah Psichologit (LAP). Agents trained in computers and engineering staff the Technology Department. The department extracts data from stolen, damaged, or foreign information systems, while ensuring the security of Mossad systems.

Little is known publicly about Mossad's final department, the Special Operations Division, also known as Metsada. The group has the tacit permission to carry out

assassinations and acts of sabotage against confirmed threats to Israel.

**Shabak.** Shin Bet, or Shabak, conducts counterintelligence and internal security operations for the Israeli intelligence community. The agency focuses on domestic and regional intelligence operations, but maintains a network of personnel worldwide.

Three internal departments aid Shabak operations. The Arab Affairs Department maintains information on Arab terrorist networks, and conducts anti-terrorism operations. The Non-Arab Affairs department concerns itself with other nations, with special attention paid to Russia and Eastern Europe. Both agencies operate within Israel and abroad. The third Shabak department, Protective Security, is responsible for the protection of Israeli diplomatic missions abroad, as well as internal security at military, government, industrial, and scientific installations within Israel's borders.

Shabak is also a political espionage agency. The agency monitors extremist political groups. Scrutiny and surveillance of the political associations of foreigners living within Israel is an additional routine Shabak activity. The agency also possesses the authority to arrest and detain persons suspected of anti-government activity. The



government attempted to keep the actions of Shabak from public view, but increased incidents of suspected brutality drew attention to agency operations in the 1980s. Despite a series of highly-publicized investigations that brought to light suspected Shabak practices (such as coercion, torture, and lying to the courts) the agency maintains the tacit consent of the Israeli government to employ special measures, including physical intimidation, to elicit information deemed urgently needed to protect Israeli security.

**Aman.** Israel's military intelligence community consists of numerous tactical intelligence units maintained by the individual branches of the Israeli Defense Force. A central agency collates, processes, and disseminates military intelligence information, as well as coordinates interagency operations. The Aman is an independent service, a peer of the army, navy, and air force. The agency produces reports for military and government use, acts as liaison between the military and government, coordinates the flow of information between civilian and military intelligence agencies, and assesses the threat of war.

Two sub-departments within the Aman assist agency operations. The Foreign Relations Department is the agency liaison with foreign military commanders and military intelligence services. The Sayeret Maktal, or Deep Reconnaissance Unit, conducts counter-terrorism operations.

## Israeli State Security Today

Israel and its Arab neighbors entered into extensive peace negotiations in the 1990s. The U.S. president and secretary of state moderated peace talks between the Israelis and the Palestinians. On October 26, 1994, long-standing territorial disputes between Israel and Jordan were settled with the signing of the Israeli-Jordanian Treaty of Peace. The following year, an Israeli right-wing extremist who opposed peace negotiations with Arab states, assassinated Israeli Prime Minister Yitzhak Rabin, a driving force in the Israeli peace movement.

Limited progress continues to be made, with Israel withdrawing from Lebanon in 2000. Growing nationalism in Israel and Palestine, however, thwarted further negotiations. A resurgence of violence between the Palestinian Muslims and Israeli Jews in 2001 marked the beginning of the second Intifada.

The Israeli government and Palestinian Authority were set to attempt a new round of peace talks in 2003, but the outbreak of war in Iraq further polarized the two governments and postponed negotiations. In May, 2003, U.S. Secretary of State Colin Powell traveled to the Middle East to call upon the new Palestinian Prime Minister Mahmoud Abbas to disarm the militant factions that have attacked Israel. Powell also urged the Israeli government to ease its crippling blockade on Palestinian cities. Both measures are deemed vital to U.S. President George W. Bush's

peace plan that calls for an end to Palestinian-Israeli violence, and the creation of a Palestinian state by the year 2005.

### ■ FURTHER READING :

#### BOOKS:

Sacher, Howard. *A History of Israel: From Zionism to Our Time*. 2nd ed. New York: Knopf, 1996.

Thomas, Gordon. *Gideon's Spies: The Secret History of the Mossad*. New York: Griffin, 2000.

#### SEE ALSO

*Eichmann, Adolf: Israeli capture Middle East, Modern U.S. Security Policy and Interventions Palestinian Authority, Intelligence and Security*

---

## Italy, Intelligence and Security

---

Although the Italian city-states were among the most prosperous and influential political organizations during the Middle Ages and the Renaissance, the modern nation-state of Italy did not emerge until the nineteenth century. King Victor Emmanuel united the city-states and kingdoms on the Italian peninsula, and the neighboring island provinces of Sicily and Sardinia in 1861. Italy was ruled by a monarchy and parliamentary government until the 1920s when Benito Mussolini established a fascist dictatorship. Through his fascist reforms, Mussolini hoped to make Italy's more agrarian south as prosperous as its industrialized north, but his alliance with Nazi Germany thrust Italy into World War II. Italian nationalists, sympathetic to the Allies, formed partisan groups that fought the Germans and fascist secret police forces behind enemy lines until the Allies successfully invaded the Italian peninsula. After Italy's defeat, the fascist regime was replaced by a democratic government.

The Executive Committee for the Intelligence and Security Services (CESIS) maintains the Office of the Secretary General, which filters and disseminates information collected by the various branches of the Italian intelligence and security committee. The main mission of the office is to act as a liaison between the intelligence services and the government, briefing government officials on intelligence matters and threats to national security when necessary. Representatives from the Office of the Secretary General routinely brief the President of the Council of Ministers regarding intelligence policy and operations. The office also coordinates inter-agency intelligence operations and established protocol regulations for intelligence personnel.

The Service for Information and Democratic Security (SISDE), administered by the Ministry of the Interior, is Italy's main domestic intelligence agency. The organization carries out all forms of surveillance and intelligence gathering operations, using some of the most sophisticated technologies in the European intelligence community. The SISDE contains several specialized operational departments, including anti-terrorism, counterintelligence, and anti-industrial espionage forces. The SISDE is also responsible for analysis of its own intelligence information, submitting completed reports or time-critical information to the CESIS.

Italy maintains specialized, strategic intelligence units within all branches of its military. However, the military and the government also administer the Intelligence and Military Security Service (SISMI). The Ministry of Defense oversees SISMI, whose responsibilities include the collection of military-related intelligence, counterespionage, and information analysis. The organization focuses on assessing threats to military and national security, whether from foreign or domestic entities.

Law enforcement in Italy is two-tiered. The military trains and administers the national police force, the Carabinieri, which has jurisdiction throughout Italy. The military police work closely with intelligence agencies,

protecting national interests and investigating federal crimes. Provinces and municipalities maintain their own civil police.

Today, Italy is part of the expanding European Union (EU). The nation participates in the European Monetary Union, North Atlantic Treaty Organization (NATO), the United Nations (UN), and several other international organizations. In 2002, Italian representatives to the EU successfully lobbied for a proposal to create EU-managed, pan-European defense and intelligence forces.

Italy is closely allied with the United States and in 2003 supported U.S. efforts in Iraq. The Italian intelligence community aids international anti-terrorist efforts, devoting considerable resources to the ferreting-out of terrorist cells operating or distributing finances within Italy's national borders.

#### ■ FURTHER READING:

##### BOOKS:

- Richelson, Jeffrey T. *Foreign Intelligence Organizations*, 2nd ed. Cambridge, MA: Ballinger Publishing, 1994.
- Willan, Philip. *Puppet Masters: The Political Use of Terrorism in Italy*. London: Constable, 1991.



## Jaish-e-Mohammed (JEM) (Army of Mohammed)

The Jaish-e-Mohammed (JEM) is an Islamic extremist group based in Pakistan that was formed by Masood Azhar upon his release from prison in India in early 2000. The group's aim is to unite Kashmir with Pakistan. It is politically aligned with the radical political party, Jamiat-i Ulema-i Islam Fazlur Rehman faction (JUI-F). The United States added JEM to the Foreign Terrorist Organization list as well as the list kept by the U.S. Treasury Department's Office of Foreign Asset Control (OFAC), which includes organizations that are believed to support terrorist groups and have assets in U.S. jurisdiction that can be frozen or controlled. The group was banned and its assets were frozen by the Pakistani government in January 2002.

**Organization activities.** The JEM's leader, Masood Azhar, was released from Indian imprisonment in December 1999, in exchange for 155 hijacked Indian Airlines hostages. The 1994 HUA kidnappings by Omar Sheikh of U.S. and British nationals in New Delhi and the July 1995 HUA/Al Faran kidnappings of Westerners in Kashmir were two of several previous HUA efforts to free Azhar. On October 1, 2001, the JEM claimed responsibility for a suicide attack on the Jammu and Kashmir legislative assembly building in Srinagar that killed at least 31 persons, but later denied the claim. The Indian government has publicly implicated the JEM, along with Lashkar-e-Tayyiba for an attack on the Indian Parliament that killed nine and injured 18.

JEM is based in Peshawar and Muzaffarabad, but members conduct terrorist activities primarily in Kashmir. They have several hundred armed supporters located in Azad Kashmir, Pakistan, and in India's southern Kashmir and Doda regions, including a large cadre of former Harakat

ul-Mujahidin (HUM) (Movement of Holy Warriors) members. Supporters are mostly Pakistanis and Kashmiris and also include Afghans and Arab veterans of the Afghan war. JEM uses light and heavy machine guns, assault rifles, mortars, improvised explosive devices, and rocket grenades. The JEM maintained training camps in Afghanistan until the fall of 2001.

Most of the JEM's cadre and material resources have been drawn from the militant groups Harakat ul-Jihad al-Islami (HUJI) and the HUM. The JEM had close ties to Afghan Arabs and the Taliban. Osama Bin Ladin (also known as Usama Bin Ladin) is suspected of giving funding to the JEM. The JEM also collects funds through donation requests in magazines and pamphlets. In anticipation of asset seizures by the Pakistani government, the JEM withdrew funds from bank accounts and invested in legal businesses, such as commodity trading, real estate, and production of consumer goods.

### ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001. Annual Report: On the Record Briefing. May 21, 2002. <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

### SEE ALSO

*Terrorism, Philosophical and Ideological Origins Terrorist and Para-State Organizations Terrorist Organization List, United States Terrorist Organizations, Freezing of Assets*

## Jamming.

SEE *Electronic Countermeasures.*

## Japan, Intelligence and Security

Japan is one of the oldest nations in Asia. Over the past two hundred years, the nation has struggled with its desire to retain its national culture while absorbing Western technology and economics. United by a strong imperial government, Japan waged war against its Asian neighbors for the first half of the twentieth century. The nation's defeat by Allied forces during World War II led to a period of United States occupation, rebuilding, and complete demilitarization. After decades of recovery, Japan re-emerged on the international stage as a democratized and economically robust nation.

In 1997, the Japanese government unveiled a plan for wide-scale centralization and reform of the nation's intelligence community. Hoping to consolidate the myriad of small intelligence agencies and bureaus, the plan called for the creation of super-agencies that combined military and civilian, foreign and domestic intelligence operations. Most of Japan's intelligence services are now controlled by the nation's Japanese Self-Defense Force, the Office of the Prime Minister, and the Ministry of Foreign Affairs.

Japan's central intelligence agency is the Naicho, or Cabinet Research Office. Only 100 personnel, all members of the Office of the Prime Minister, staff the agency. Naicho operations focus on the collection and analysis of foreign intelligence information, including that which is gathered by other national civilian and military intelligence forces. The agency coordinates inter-agency intelligence operations and acts as liaison between the intelligence community and the government, reporting to the prime minister and legislature when necessary.

The Bureau of Defense Policy, the government ministry which drafts Japan's defense policy and coordinates defense efforts, maintains the Jouhou Honbu, Defense Intelligence Office (DIO). The DIO is divided into two operational sections, the First and Second Intelligence Divisions. The First Intelligence Division, now known simply as the Intelligence Division, conducts domestic intelligence and security operations. Its general mission is to procure and process information relating to threats to Japan's national security. The division employs its own counterintelligence and anti-terrorism experts. The Second Intelligence Division is responsible for foreign intelligence information, and is now known as the International Planning Division.

Intelligence community reforms in the 1990s concentrated their centralization efforts on the former Defense Administration (DA). The old agency divided intelligence operations among several internal bureaus, each of which maintained their own action forces and military support

teams. The Defense Intelligence Headquarters (DIH) serves as nerve center for the new intelligence agencies that were formerly DA intelligence bureaus. The DIH conducts both foreign and domestic intelligence operations and manages various specialized sources, including human, signals, communications, and remote intelligence. The DIH also employs both civilian and military agents, and maintains its own analytics, logistics, and research force to process intelligence information.

Despite consolidation, centralization, and reform efforts, Japan's intelligence community has not yet completed its structural transformation. Many small bureaus continue to operate, and there is substantial overlap of the duties of various agencies.

Japan's economic success has made extensive counterintelligence and anti-industrial espionage measures a primary concern of the nation's domestic intelligence community. The nation's proximity to more volatile states in Southern Asia, and occasional terrorist attacks in Tokyo, prompted Japan's intelligence services to extensively cooperate with international and foreign intelligence and security organizations. Currently, Japan participates in the international initiative to combat global terrorism, and helps to monitor the proliferation of weapons in Asia.

### ■ FURTHER READING:

#### BOOKS:

- McClain, James. *Japan: A Modern History*. New York: W. W. Norton, 2002.
- Mercado, Stephen C. *The Shadow Warriors of Nakano: A History of the Imperial Japanese Army's Elite Intelligence School*. Washington, D.C.: Brassey's, 2002.

## Japanese Red Army (JRA)

The Japanese Red Army (JRA) also operates as, or is known as, the Anti-Imperialist International Brigade (AIIB).

The JRA is an international terrorist group formed around 1970 after breaking away from the Japanese Communist League-Red Army Faction. Fusako Shigenobu led the JRA until her arrest in Japan in November, 2000. The JRA's historical goal has been to overthrow the Japanese government and monarchy and to help foment world revolution. After her arrest, Shigenobu announced she intended to pursue her goals using a legitimate political party rather than revolutionary violence, and the group announced it would disband in April, 2001. JRA may

## JDAM (Joint Direct Attack Munition)

control or at least have ties to the Anti-Imperialist International Brigade (AIIB) and also may have links to the Antiwar Democratic Front—an overt leftist political organization—inside Japan. Details released following Shigenobu's arrest indicate that the JRA was organizing cells in Asian cities, such as Manila and Singapore. The group had a history of close relations with Palestinian terrorist groups—based and operating outside Japan—since its inception, primarily through Shigenobu. The current status of the connections is unknown. During the 1970s, JRA carried out a series of attacks around the world, including the massacre in 1972 at Lod Airport in Israel, two Japanese airliner hijackings, and an attempted takeover of the U.S. Embassy in Kuala Lumpur. In April, 1988, JRA operative Yu Kikumura was arrested with explosives on the New Jersey Turnpike, apparently planning an attack to coincide with the bombing of a USO club in Naples, a suspected JRA operation that killed five, including a U.S. servicewoman. Kikumura was convicted and is serving a lengthy prison sentence in the United States. Tsutomu Shirosaki, captured in 1996, is also jailed in the United States. In 2000, Lebanon deported to Japan four members arrested there in 1997, but granted a fifth operative, Kozo Okamoto, political asylum. Longtime leader Shigenobu was arrested in November 2000 on charges of terrorism and passport fraud.

The JRA has about six dedicated members and an undetermined number of sympathizers. At its peak, the group claimed to have 30 to 40 members. The exact location of JRA is unknown, but intelligence estimates indicate that it possibly operates in Asia and/or Syrian-controlled areas of Lebanon.

### ■ FURTHER READING:

#### ELECTRONIC:

CDI (Center for Defense Information), Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <<http://www.cdi.org/terrorism/terrorist.cfm>> (April 17, 2003).

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001." Annual Report: On the Record Briefing. May 21, 2002. <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

#### SEE ALSO

*Terrorism, Philosophical and Ideological Origins Terrorist and Para-State Organizations Terrorist Organization List, United States Terrorist Organizations, Freezing of Assets*

The Joint Direct Attack Munition (JDAM) is a satellite-guided "smart" bomb capable of accurate and high-precision strikes in any weather. JDAM munitions have found increasing use in military missions and the use of precision bombs exceeded 80 percent in the U.S.-led Operation Iraqi Freedom conducted in 2003. Because of their high degree of accuracy, JDAM munitions can also be used to selectively strike at intelligence-related targets, and in the Iraq campaign, they were used to strike at military and intelligence (e.g. leadership targets) that Saddam Hussein's forces had placed or attempted to conceal in or near civilian areas.

JDAM munitions also found wide use in the NATO air campaign against the Federal Republic of Yugoslavia in 1999 and in the 2001 U.S.-led Operation Enduring Freedom against the Taliban regime and al-Qaeda forces hiding in Afghanistan. As of April 2003, U.S. B-1, B-2, B-52, F-16 and F/A-18 bombers and fighter/strike aircraft were capable of carrying JDAM munitions.

JDAM munitions are intended to provide accurate delivery of general purpose bombs in adverse weather conditions. Although not quite as accurate as laser-guided munitions, JDAM offer high precision—but at a far lower cost than laser-guided munitions. JDAMs are dumb bombs converted to smart bombs by the supplemental addition of fixed aerodynamic surfaces (mid-body strakes and tail fins) and a guidance package that allows inertial navigational guidance of the bomb following release. Targeting is maintained via continuously updated global positioning satellite (GPS) data that steers the bomb to the target. Under normal conditions, JDAMs can determine location and strike within 10 yards of an intended target. Because they rely on GPS signals, JDAMs can be used even under cloudy conditions, or when the sky is obscured by smoke.

Jamming equipment that can scramble or block GPS signals has limited effectiveness against JDAM munitions because the tracking sequence is progressive (i.e., the jamming is not effective until the bomb is almost on target) and software corrections allow the bombs to revert to inertial navigation if the GPS signal is blocked or obscured. In general, Iraqi forces using Russian-made jamming equipment found little success in reducing JDAM precision. Although detailed assessments were not yet complete as of May 2003, Iraqi attempts at jamming JDAMs—intended for precision strikes at military targets hidden near civilian areas—may have accounted for some unintended civilian casualties.

Other significant JDAM misses include the accidental bombing of the Chinese embassy by a JDAM released by a U.S. B-2 bomber over Belgrade in May 1999. The bombing

killed three Chinese citizens. That targeting error was not a result of jamming but was attributed to a software error that relied on outdated maps.

#### ■ FURTHER READING:

##### ELECTRONIC:

Federation of American Scientists. Military Analysis Network. Joint Direct Attack Munition (JDAM) GBU-29, GBU-30, GBU-31, GBU-32. September 18, 2002. <<http://www.fas.org/man/dod-101/sys/smart/jdam.htm>> (April 15, 2003).

##### SEE ALSO

*Iraqi Freedom, Operation (2003 War Against Iraq)*

---

## Jemaah Islamiya (JI)

---

Jemaah Islamiya (JI) is an Islamic extremist group with cells operating throughout Southeast Asia. Members arrested in Singapore, Malaysia, and the Philippines have revealed links with al-Qaeda. The JI's stated goal is to create an Islamic state comprising Malaysia, Singapore, Indonesia, and the southern Philippines. Three Indonesian extremists, one of whom is in custody in Malaysia, are the reported leaders of the organization. JI began developing plans in 1997 to target U.S. interests in Singapore and, in 1999, conducted videotaped casings of potential U.S. targets in preparation for multiple attacks in Singapore. A cell in Singapore acquired four tons of ammonium nitrate, which has not yet been found. In December 2001, Singapore authorities arrested 15 Jemaah Islamiya members—some of whom had trained in al-Qaeda camps in Afghanistan—who planned to attack the U.S. and Israeli embassies and British and Australian diplomatic buildings in Singapore. Additionally, the Singapore police discovered forged immigration stamps, bomb-making materials, and al-Qaeda-related material in several suspects' homes.

The exact numbers of JI are unknown but press reports approximate that the Malaysian cells may comprise 200 members. The JI has cells in Singapore and Malaysia; press reports indicate the JI is also present in Indonesia and possibly the Philippines.

In October 2002, a bomb destroyed a nightclub in Bali, Indonesia, killing 202 people. In August 2003, an Indonesian court convicted and sentenced to death a member of the Islamist militant group Jemaah Islamiyah for helping plan the attack. Although one-half of the people killed in the Bali attack were vacationing Australians, the convicted

terrorist claimed subsequently through his lawyer that "the targets were the Americans and the Jews."

#### ■ FURTHER READING:

##### ELECTRONIC:

CDI (Center for Defense Information), Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <<http://www.cdi.org/terrorism/terrorist.cfm>> (April 17, 2003).

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001." Annual Report: On the Record Briefing. May 21, 2002. <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

##### SEE ALSO

*Terrorism, Philosophical and Ideological Origins  
Terrorist and Para-State Organizations  
Terrorist Organization List, United States  
Terrorist Organizations, Freezing of Assets*

---

## Johnson Administration (1963–1969), United States National Security Policy

---

#### ■ CARYN E. NEUMANN

President Lyndon B. Johnson continued the longstanding commitment of the United States to Southeast Asian security by providing increasing amounts of support to anti-communist South Vietnam. A former congressman from Texas and vice-president since 1960, Johnson took office in 1963 upon the assassination of President John F. Kennedy. In light of the circumstances, Johnson considered it his obligation to the electorate to continue Kennedy's policies. He stated his determination to resist Soviet expansionism and reiterated the nation's support of South Vietnam.

Johnson also moved national security policy in the direction that Kennedy had indicated. Kennedy allowed the structure of the National Security Council to atrophy and Johnson continued to this process. Congress had established the NSC as a means of encouraging the president to consider political and military advice, but the men

in the Oval Office did not always cooperate with the plans of the legislative branch. Both leaders sought greater direct presidential control over foreign relations.

Johnson generally operated outside the formal advisory structure of the NSC. He saw the council as too large and unwieldy to serve as a forum for policy formulation. Perhaps more significantly, the Johnson NSC also established a reputation as a major source of leaks to the news media and to Capitol Hill. With the president holding the NSC at arm's length and treating it as only a symbolic mechanism, the frequency of its meetings declined during his administration. The president generally used the council as a means of informing subordinates about the future direction of policy.

For national security advice, the Johnson administration depended chiefly upon the national security advisor (NSA). This role was filled by McGeorge Bundy, Kennedy's NSA who remained in office through February 1966, and Bundy's successor, economist Walt Rostow, who served to the end of the administration. The NSA staff, various ad hoc groups, and trusted friends also offered assistance. In 1966, Johnson officially turned over responsibility for the supervision and coordination of interdepartmental activities overseas to Secretary of State Dean Rusk. Kennedy's Secretary of Defense Robert McNamara continued to fill that role under Johnson.

While serving under Kennedy, McNamara began to develop a doctrine of mutual assured destruction (MAD) that he honed under Johnson. According to MAD, deterrence depended upon the confidence of each superpower in the ability of its own nuclear forces to survive a first attack and retaliate. Mutual fear of massive deaths among the populace served as an incentive to avoid making that first strike.

As MAD indicates, potential nuclear conflict dominated the administration's treatment of the Soviet Union. Warnings by McNamara about the suicidal arms race that both nations were running helped persuade Johnson to agree to a nuclear nonproliferation treaty. In 1968, each power pledged to halt the distribution of nuclear weapons. While 59 other nations also signed the treaty, not every country agreed; China, France, and India refused to participate.

Johnson sought to de-escalate Cold War rhetoric, but continued to see the Russians as a threat that had to be contained and this objective would lead to the escalation of involvement in Vietnam. As did the presidents before him, Johnson struggled to find a means to save South Vietnam from communist aggression. A brief and confusing episode between North Vietnamese and American naval forces in the Tonkin Gulf in 1964 gave Johnson his opportunity. He used the incident to secure a resolution from Congress giving him authority to employ armed forces to defend American personnel in South Vietnam and stop further attacks.

Johnson used the resolution as his authority to wage war in Southeast Asia. A supporter of the domino theory,

Johnson held that if South Vietnam fell to communism, then the other free governments in the region would also topple, thereby costing the U.S. its valuable Asian allies. Under Johnson, the American military commitment to Vietnam rose rapidly to a force that peaked at 543,000 in 1969.

Protests against the war grew slowly. In 1966, Senator J. William Fulbright, head of the Senate Foreign Relations Committee began nationally televised hearings on American national security policy. Fulbright, a powerful Arkansas Democrat, argued that by escalating the war, Johnson had exceeded the limits of the authority granted to him by Congress in the Tonkin Gulf Resolution. Witness George Kennan, a top State Department expert on Russia who had helped shape Truman's doctrine of containment, challenged testimony by Secretary of State Rusk that the U.S. had to fight in Vietnam to prevent Soviet expansion. Kennan argued that the conflict in Vietnam had so preoccupied the government that areas of more important strategic significance had been stripped of forces sufficient to deter a possible Soviet attack. The hearings indicated deep divisions over foreign policy.

During 1966, increasing numbers of members of the Johnson administration spoke out against the Vietnam War. Unable to brook dissent, Johnson did not tolerate attacks on his policy. His intolerance of criticism persuaded some of his most trusted national security counselors, including NSA Bundy and George Ball of the State Department, to leave government service. Whereas Bundy had informed Johnson of the full range of senior opinions about national security, Rostow gave hawkish advice. Increasingly isolated from contrary opinions, Johnson had established an administration with little dissenting opinion.

Throughout 1967, doubts about the Vietnam War consumed additional members of the government. Both Secretary of Defense McNamara and the Central Intelligence Agency challenged the judgment of the military. While the Joint Chiefs sought intensified bombing of North Vietnam, McNamara had concluded that massive bombing only boosted patriotism in that country instead of destroying the will of its people to fight. After McNamara categorized administration policy as dangerous, expensive, and failed, Johnson decided to replace him, and McNamara left in 1967. His successor, Clark Clifford, a longtime Democratic party stalwart who had helped establish the NSC, finally managed to persuade Johnson that Vietnam could not be won. Johnson did not run for reelection.

The Johnson administration's national security policy strained the resources of the U.S. and made it difficult for succeeding presidents to mobilize support for military security efforts. Besides eroding American military effectiveness, Johnson's failed effort in Vietnam raised doubts about the nation's willingness to use military power to support its foreign policy of deterring the spread of communist governments abroad.

## ■ FURTHER READING :

### BOOKS:

Boll, Michael M. *National Security Planning: Roosevelt Through Reagan*. Lexington: University Press of Kentucky, 1988.

Crabb, Cecil V., and Kevin V. Mulcahy. *American National Security: A Presidential Perspective*. Pacific Grove, CA: Brooks/Cole, 1991.

Hunt, Michael H. *Lyndon Johnson's War: America's Cold War Crusade in Vietnam, 1945–1968*. New York: Hill and Wang, 1996.

### ELECTRONIC:

White House. "History of the National Security Council, 1947–1997." <<http://www.whitehouse.gov/nsc/history.html>> (April 25, 2003).

### SEE ALSO

*CIA (United States Central Intelligence Agency) Cold War (1950–1972)*

*Joint Chiefs of Staff, United States*

*National Security Advisor, United States*

*NSC (National Security Council)*

*NSC (National Security Council), History*

*National Security Strategy, United States*

*Nonproliferation and National Security, United States Vietnam War*

## Joint Chiefs of Staff, United States

### ■ JOSEPH PATTERSON HYDER

The Joint Chiefs of Staff (JCS) of the United States is a six-member committee that advises the president, the secretary of defense, and the National Security Council on military affairs. A chairman, vice-chairman, and the chiefs of each of the four branches of the military form the Joint Chiefs of Staff. The chief of each military branch also serves as manager of his military branch, although these management duties typically fall to the vice-chief. The chairman conducts meetings of the JCS and serves as the primary military advisor to the President.

The Joint Chiefs of Staff was formed following the Arcadia Conference in 1942, during which President Franklin D. Roosevelt and United Kingdom Prime Minister Winston Churchill formed the Combined Chiefs of Staff to conduct the war effort on behalf of the United States and Britain. The Combined Chiefs of Staff consisted of senior members of the American and British armed forces. While the British established a Joint Chief of Staff Committee in 1924 in order to advise the Prime Minister and War Cabinet, the United States did not have a central military

command in place to contribute a coordinated military plan to the Combined Chiefs. U.S. Admiral William Leahy led an effort to establish an American unified high command. The result of Admiral Leahy's efforts was the formation of the Joint Chiefs of Staff, of which he was named Chief of Staff to the Commander in Chief of the Army and Navy.

During World War II, Roosevelt granted great latitude to the actions of the Joint Chiefs of Staff. During the war, the Joint Chiefs acted as executive commanders of troops in the field, answering only to the President. The National Security Act of 1947 formally established the Joint Chiefs of Staff and defined the roles of the chiefs as that of advisers to the President and not as commanders with executive authority.

Despite the statute prohibiting the chiefs from commanding forces, the chief of each armed service branch continued to act with executive authority in originating contact with combat commanders, thus violating the spirit of the National Security Act of 1947. Congress amended the National Security Act in 1953 to prevent such contact with field commanders.

The Goldwater-Nichols Department of Defense Reorganization Act of 1986 further redefined the function of the Joint Chiefs of Staff. This act went beyond the National Security Act in terms of expressly stating the role of the executive authority in relation to the Joint Chiefs of Staff. The Goldwater-Nichols Act mandated that the chain of command run from the President to the Secretary of Defense to the combatant commanders. The chairman of the Joint Chiefs of Staff may transmit orders to commanders from either the President or the Secretary of Defense, but the Chairman may not exert executive authority or command troops.

The act also defined other functions that the chairman may perform. The chairman may consult with the other chiefs and with commanders in the field but may not commit or command forces. He must then present the advice that he receives to the president, secretary of defense, or National Security Council. All members of the Joint Chiefs of Staff are presidential advisers and may submit their opinions to the president through the chairman.

The Goldwater-Nichols Act also established the position of vice-chairman. The vice-chairman conducts meetings of the Joint Chiefs in the absence of the chairman and carries out duties as stipulated by the chairman. Originally the vice-chairman was not a full, voting member of the Joint Chiefs of Staff. The National Defense Authorization Act of 1992 granted the vice-chairman full status, increasing the Joint Chiefs of Staff to six members.

## ■ FURTHER READING :

### ELECTRONIC:

United States Department of Defense. "JCS Link, The Joint Chiefs of Staff." <<http://www.dtic.mil/jcs/>> (May 5, 2003).





The Joint Chiefs of Staff pose together in an official photograph in the Joint Chiefs of Staff Gold Room at the Pentagon, January 11, 2000. ©REUTERS NEWMEDIA INC./CORBIS.

#### SEE ALSO

*DOD (United States Department of Defense)*  
*NSC (National Security Council)*

## Jordan, Intelligence and Security

The primary Jordanian intelligence agency is the *Dairat al Mukhabarat*, or General Intelligence Department (GID). The GID is charged with the collection and analysis of intelligence information. GID officials brief the government on matters of national security and coordinate efforts with the military and national law enforcement agencies. The focus of GID operations is the collection of

intelligence pertaining to security issues within the Middle East, including surveillance of paramilitary groups and guarding borders to prevent an influx of refugees from the neighboring area of Palestine. The GID also provides the government with regular reports of the political climate of the nation and the surrounding region, though the means by which this information is gathered remains secret.

Because the Jordanian intelligence community is consolidated into one major agency, the GID maintains several special task forces devoted to specialized areas of intelligence, including counter-intelligence and communications surveillance. An anti-terrorism task force conducts operations to gather information on organizations working in Jordan and throughout the Middle East. The Jordanian government has aided international anti-terrorism efforts following the September 11 terrorist attacks on the United States. The government also employs GID staff



The car belonging to the wife of a senior anti-terrorism official in Jordan was destroyed in a February 2002, explosion in response to Jordan's support for the U.S.-led campaign against terrorism. AP/WIDE WORLD PHOTOS.

to monitor the security of government information systems and personnel. Security surveillance of the government also includes an anti-corruption department to root out incidences of government abuse. Economic, industrial, scientific, and limited political espionage is also conducted by GID forces.

During the Persian Gulf War in 1991, Jordan was the only Arab country that did not openly condemn the Iraqi invasion of Kuwait. However, the Jordanian government did not provide aid to the Iraqi government during the war and tried to maintain diplomatic relations with both Israel and the United States. Jordan opposed coalition military involvement in Iraq again in 2003, but permitted United States and British forces to use Jordan's airspace and bases for some operations. Jordan's monarchy and government continues to walk a tightrope in Middle East politics, signing a formal peace treaty with Israel in 1994 and fostering favorable diplomatic relations with the West, even though the majority of the nation's Arab population opposes both policies.

#### FURTHER READING:

#### ELECTRONIC:

Intelligence Services of Jordan. <<http://www.gid.gov.jo/>> (March 28, 2003).

#### SEE ALSO

*Iraqi Freedom, Operation (2003 War Against Iraq)*  
*Persian Gulf War*

## J-STARS

J-STARS (Joint Surveillance and Target Acquisition Radar System) is the name for a type of surveillance aircraft developed jointly by the U.S. Army and Air Force. Adapted from the Boeing 707-320, the aircraft itself—on which both Boeing and Grumman worked as contractors—is designated the E-8. Its capabilities include sophisticated radar systems that allow it to conduct extensive ground surveillance.

For the better part of two decades, the air force had sought to develop an aircraft with improved radar capabilities, and in 1985 it began these efforts in earnest by joining forces with the army to create such a plane. The result was J-STARS, whose most notable feature is the pod or radome under the forward fuselage measuring

some 24 feet (7.3 m) and shaped like a canoe; it contains a radar system capable of detecting targets the size of a truck over an area of 200 square miles (518 sq km).

Whereas aircraft have long had radar systems to track other planes and stationary objects, the uniqueness of J-STARS lay not only in the fact that its radar monitored activity on the ground, but that it did so with unparalleled precision. J-STARS made it possible to monitor literally hundreds of stations at the same time, using high-resolution imaging.

Two E-8A prototype J-STARS made their initial flight on April 1, 1988, and these two later saw service in Operation Desert Storm during January 1991. Flown on 49 combat sorties for a total of 500 combat hours, the aircraft displayed almost flawless effectiveness in tracking mobile Iraqi ground forces, tanks, and Scud missiles.

J-STARS again saw service during Operation Joint Endeavor, a North Atlantic Treaty Organization (NATO) action in Bosnia to monitor compliance with the Dayton Peace Treaty agreements in December 1995. The E-8A test craft, as well as the pre-production E-8C model, logged more than 1,000 flight hours on 98 sorties, with a 98 percent effectiveness rate. J-STARS have also been used in NATO's Operation Allied Force in March to June 1999 over Kosovo, and in the U.S. Operation Enduring Freedom in Afghanistan in October 2001.

#### ■ FURTHER READING:

##### BOOKS:

Polmar, Norman, and Thomas B. Allen. *Spy Book: The Encyclopedia of Espionage*. New York: Random House, 1998.

##### PERIODICALS:

Babbin, Jed. "Some Things Can't Wait: Speedy Approval of New Military Technologies Will Save Lives." *Washington Times*. (June 27, 2002): A23.

##### ELECTRONIC:

Grumman/Boeing E-8 J-STARS. <<http://www.zap16.com/mil%20fact/e-8%20j-stars.htm>> (January 22, 2003).

##### SEE ALSO

*Persian Gulf War*  
RADAR

protecting the interests of the nation in legal matters. Created in 1870, it is directed by the attorney general, the nation's chief law enforcement officer, whose office long predates the department itself. Under the aegis of the Justice Department are a number of prominent law enforcement bureaus and agencies, including the Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA), United States Marshal Service (USMS), and many others. Another prominent Justice agency, the Immigration and Naturalization Service (INS), became part of the Department of Homeland Security in 2003. In the twenty-first century, key areas of concern for Justice are terrorism, worldwide drug trafficking, community violence, white collar crime, substance abuse, and hate crimes.

**History.** In 1789, the first Congress passed the Judiciary Act, which established the federal justice system and created the Office of the Attorney General. A member of the cabinet without his own executive department, the attorney general advised the president on legal matters and represented the federal government before the Supreme Court. Among the prominent attorneys general of those early years were Roger B. Taney (1831–33), who later became one of the most notable chief justices of the Supreme Court, and Edwin M. Stanton (1860–61), who became Secretary of War under President Abraham Lincoln.

In 1870, Congress created the Department of Justice, and placed all existing federal law enforcement agencies—for example, USMS, also created by the 1789 Judiciary Act—under the new department. Its head would be the attorney general, and its second-highest office would be that of solicitor general, whose job it is to supervise and conduct government litigation before the Supreme Court. Prominent solicitors general included future president William Howard Taft (1890–92); future Supreme Court justices Charles Evans Hughes, Jr. (1929–30) and Thurgood Marshall (1965–67), who was also the first African American solicitor general; Archibald Cox (1961–65), Robert Bork (1973–77), and Kenneth Starr (1989–93).

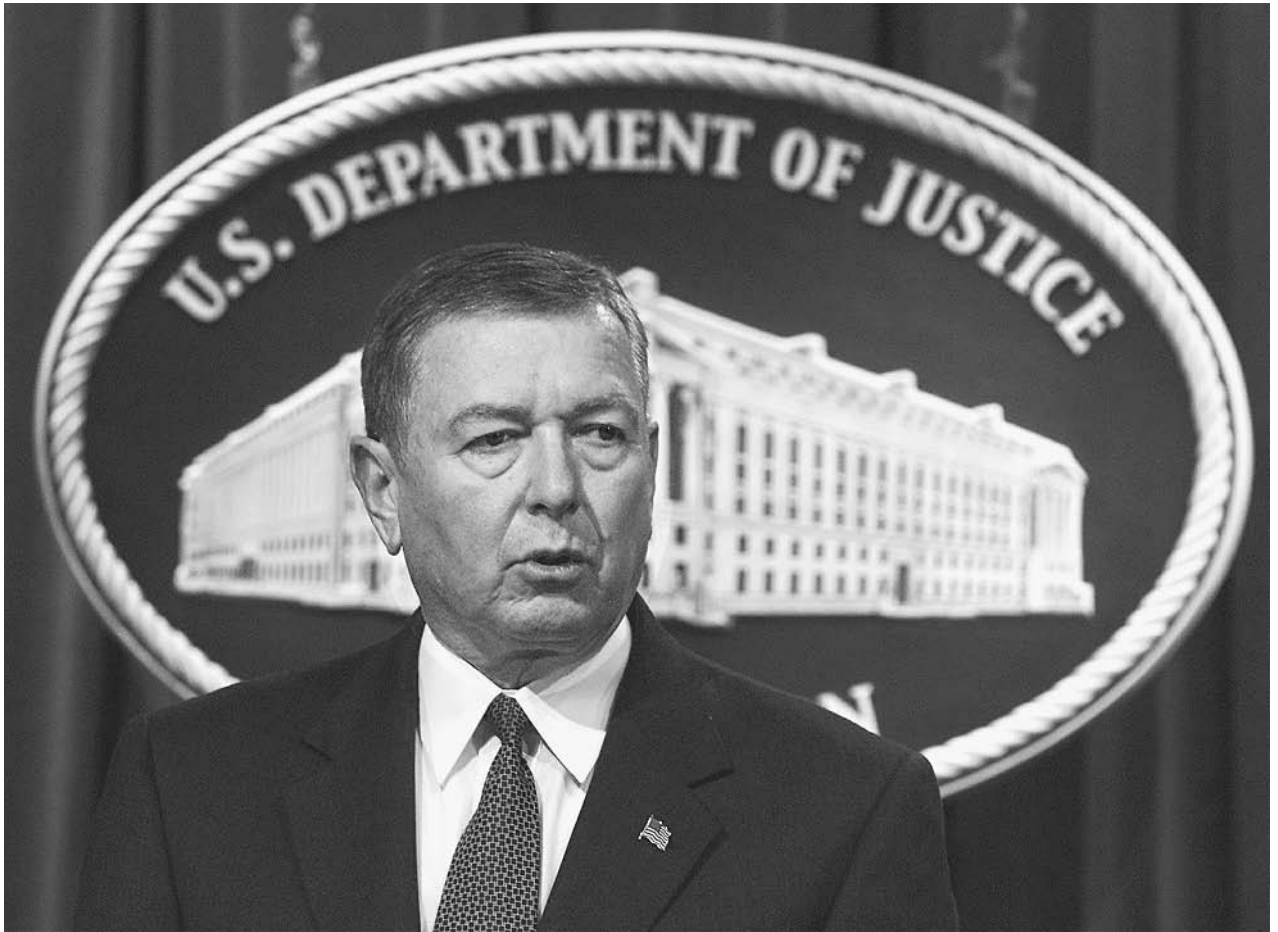
Among the notable attorneys general since 1870 were A. Mitchell Palmer (1919–21), a leading figure in the post-World War I "Red Scare"; future Supreme Court Chief Justice Harlan Fiske Stone (1924–25); Robert F. Kennedy (1961–64); Ramsey Clark (1967–69), noted for his later involvement in protest movements and highly publicized court cases; John N. Mitchell (1969–72) and a host of other attorneys general associated in some way with the Watergate scandal; and Janet Reno (1993–2001), first female attorney general.

**Mission, agencies, and activities.** The mission of the Department of Justice is to enforce the law and defend the interests of the United States according to law; to provide federal leadership in preventing and controlling crime; to seek just punishment for those found guilty of unlawful acts; to administer and enforce the nation's immigration

## Justice Department, United States

#### ■ JUDSON KNIGHT

The U.S. Department of Justice is responsible for enforcing federal law, preventing and controlling crime, and



Attorney General John Ashcroft briefs reporters at a press conference at the Justice Department in Washington, D.C., on October 29, 2001, as the FBI issued a new terrorism warning asking Americans and law enforcement to be on the highest alert for possible attacks in the United States and abroad. AP/WIDE WORLD PHOTOS.

laws fairly and effectively; and to ensure fair and impartial administration of justice for all Americans.

The Justice Department accomplishes that mission through a vast array of activities. In addition to the FBI and DEA, prominent agencies include the Bureau of Alcohol, Tobacco, Firearms, and Explosives (part of the Treasury Department until 2002); the Federal Bureau of Prisons and its National Institute of Corrections, which are responsible for the incarceration of sentenced offenders; the U.S. National Central Bureau of Interpol; and USMS, which is responsible for protecting federal courts and ensuring the effective operation of the judicial system. Long celebrated in story and legend, U.S. marshals pursue 55 percent of all federal fugitives, more than all other federal agencies combined.

The Justice Department conducts legal actions against violations of federal antitrust laws through its Antitrust Division, and violations of civil rights laws through its Civil Rights Division. Its Civil Division represents federal interests in civil litigation, while the Criminal Division develops, supervises the application of, and even enforces

federal criminal statutes not covered by other agencies. The Asset Forfeiture Program handles money and other goods involved in criminal activities.

Through sections such as the Community Oriented Policing Services (COPS) and the Office of Justice Programs (which includes numerous bureaus such as the American Indian and Alaska Native Affairs Desk), the Department of Justice maintains state, municipal, and community outreach activities designed to reduce crime and crime-related behaviors, and encourage citizen involvement in crime prevention. It maintains databases on criminal activity through the Bureau of Justice Statistics and the National Drug Intelligence Center. The National Institute of Justice develops and disseminates studies on issues related to crime and justice.

The Justice Department *Strategic Plan*, released late in 2001, discussed the challenges and opportunities faced by the department at the beginning of the twenty-first century. Whereas crime rates had gone down from the 1930s to the 1960s, in the latter decade they had begun to climb, and continued to do so until the mid-1990s. The

period after the mid-1990s, however, saw a steady reduction in criminal activity nationwide.

The report credited more coordinated national policing efforts in the wake of the congressional passage of the Safe Streets Act in 1968. This had led to increased financial assistance for law enforcement at the federal, state, and local levels, resulting in the development of agencies that were better prepared to meet the challenges of their environments.

Additionally, since the late 1980s, criminal and juvenile justice agencies had increasingly partnered with community-based organizations such as schools, churches, businesses, social services, and victim advocacy groups. In 1984, the Victims of Crime Act established an Office for Victims of Crime in the Justice Department, even as numerous national and community-based organizations were formed to provide support to victims of rape, spousal abuse, drunk driving, and other crimes.

The Justice Department was given broader authority to enforce federal law against criminal organizations, including gangs, criminal syndicates, and terrorists. During the mid-1990s, the Brady Handgun Violence Prevention Act and the establishment of a National Instant Criminal Background Check System had helped bring about a steady decrease in gun-related crimes. The Sentencing Reform Act of 1984 greatly stiffened prison sentences, requiring mandatory terms for certain crimes and abolishing federal parole. These changes, along with more aggressive enforcement measures, led to an increase in the number of incarcerated persons, which reached an all-time high of 1.8 million detainees in 1999.

**From the present to the future** Among the notable aspects of the early twenty-first century law enforcement environment noted in the report were globalization and advances in science and technology. The terrorist attacks of September, 2001, had dramatically illustrated the international scope of criminal activity, but the Justice Department had also increasingly taken a multinational approach, working with Interpol and other groups overseas.

Similarly, advances in information technology made possible new opportunities for crimes involving fraud, theft of intellectual property, and child pornography, while

scientific advances in the use of DNA evidence and other forensic technology provided a boost to law-enforcement activities. Other technologies noted in the Justice Department report were advances in biotechnology and bioengineering (most notably the decoding of the human genome), and nanotechnology, or the ability to manipulate matter at the molecular or even atomic levels.

Leading the list of key concerns for the coming years, of course, was terrorism, followed by its close cousin, worldwide drug trafficking. Other significant criminal areas include white collar and economic crimes such as health-care fraud, as well as hate crimes and crimes involving infringement of victims' civil rights.

#### ■ FURTHER READING:

##### BOOKS:

*200th Anniversary of the Office of the Attorney General, 1789–1989.* Washington, D.C.: Department of Justice, 1991.

*The Department of Justice Manual.* Gaithersburg, MD: Aspen Law & Business, 2000.

Moriarty, Laura J., and David L. Carter. *Criminal Justice Technology in the 21st Century.* Springfield, IL: Charles C. Thomas, 1998.

Riley, Kevin Jack, and Bruce Hoffman. *Domestic Terrorism: A National Assessment of State and Local Preparedness.* Santa Monica, CA: RAND Corporation, 1995.

##### ELECTRONIC:

U.S. Department of Justice. <<http://www.usdoj.gov/>> (April 14, 2003).

##### SEE ALSO

*ATF (United States Bureau of Alcohol, Tobacco, and Firearms)*

*Commission on Civil Rights, United States*

*DEA (Drug Enforcement Administration)*

*Domestic Preparedness Office (NDPO), United States National*

*FBI (United States Federal Bureau of Investigation)*

*INS (United States Immigration and Naturalization Service)*

*Interpol (International Criminal Police Organization)*

*NDIC (Department of Justice National Drug Intelligence Center)*

*NIJ (National Institute of Justice)*

*Terrorist Organizations, Freezing of Assets*

*This page intentionally left blank*



---

## Kahane Chai (Kach)

---

Kahane Chai's (Kach) stated goal is to restore the biblical state of Israel. Kach (founded by radical Israeli-American rabbi Meir Kahane) and its offshoot Kahane Chai, which means "Kahane Lives" (founded by Meir Kahane's son Binyamin following his father's assassination in the United States), were declared to be terrorist organizations in March 1994, by the Israeli Cabinet under the 1948 Terrorism Law. This followed the groups' statements in support of Dr. Baruch Goldstein's attack in February 1994 on the al-Ibrahimi mosque. Goldstein was affiliated with Kach and their verbal attacks on the Israeli government. Palestinian gunmen killed Binyamin Kahane and his wife in a drive-by shooting in December 2000 in the West Bank.

Kach organizes protests against the Israeli government, harasses and threatens Palestinians in Hebron and the West Bank. Members have threatened to attack Arabs, Palestinians, and Israeli government officials. Additionally, Kach members have vowed revenge for the death of Binyamin Kahane and his wife.

The size of Kach is unknown. They operate in Israel and West Bank settlements, particularly Qiryat Arba' in Hebron, and the group receives support from sympathizers mostly in the United States and Europe.

### ■ FURTHER READING :

#### ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001. Annual Report: On the Record Briefing. May 21, 2002. <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

### SEE ALSO

*Terrorism, Philosophical and Ideological Origins*  
*Terrorist and Para-State Organizations*  
*Terrorist Organization List, United States*  
*Terrorist Organizations, Freezing of Assets*

---

## Kennedy Administration (1961–1963), United States National Security Policy

---

### ■ CARYN E. NEUMANN

President John F. Kennedy entered the White House with confidence that instability in the developing world posed the greatest risk to the national security of the United States. Kennedy planned to resist Soviet expansionism in Latin America, Asia, and Africa by abandoning Eisenhower's policy of massive retaliation in favor of a flexible response, combining economic support with military assistance.

Aggressive and eager to prove himself, Kennedy viewed the Cold War as a struggle of good against evil that required tough action. Through his experiences of World War II, Kennedy held that democracies tended to move too slowly to oppose totalitarianism. He also took note of the narrow margin of victory that had brought him to power and allowed it to shape his security policy. Kennedy tended to defer to military and intelligence experts who favored military action rather than pursue negotiations that would be harder to sell to the American public.



During the Cuban Missile Crisis in October 1962, President John F. Kennedy meets with his cabinet and advisors at the White House. ©BETTMANN/CORBIS.

Kennedy's confrontational style did not mesh with the quiet negotiating habits of diplomats in the State Department, and the agency subsequently lost some influence in the White House. The National Security Council (NSC) under adviser McGeorge Bundy increasingly served as an alternate source of policy development and advice at the expense of the State Department under Dean Rusk. This NSC was a far different construct than the one that had served Eisenhower, but it remained focused almost exclusively on foreign policy matters.

While Kennedy would probably have eventually dismantled the elaborate Eisenhower-era NSC in favor of a more open system, the Senate gave him a push. In 1960, the Senate Subcommittee on National Policy Machinery, popularly known as the Jackson Subcommittee for its chairman Senator Henry Jackson, charged that the NSC had been rendered virtually useless by ponderous, bureaucratic machinery. The formality of the NSC system forced the continuation of established policies rather than the generation of new ideas. Heavily influenced by this

report, Kennedy deliberately snuffed out the distinction between planning and operation that had governed Eisenhower's NSC, holding that security policy is much more affected by day-to-day events than by any long term planning effort. Kennedy adopted a collegial style of decision-making in which information flows to the president from several competing sources rather than through one bureaucratic process.

The first serious security problem that confronted Kennedy involved intelligence about a purported missile gap between the U.S. and the Soviet Union. The missile gap controversy, which dominated the national security debates of the late 1950s and early 1960s, arose from the fear that the Soviets would possess a commanding superiority in intercontinental ballistic missiles (ICBMs) in just a few years. Both Soviet braggadocio and the American military services encouraged this idea of a missile gap. Two centuries of America's near imperviousness to direct attack appeared at an end. When Kennedy entered office, he discovered the gap was a myth. In order to avoid future



self-serving use of intelligence estimates by the military, Secretary of Defense Robert McNamara set up the Defense Intelligence Agency to centralize intelligence.

During Kennedy's three years in office, he would work closely with McNamara to supervise the largest and most rapid buildup of military forces in the peacetime history of the U.S. Designed to serve as a deterrent, the buildup provided the nation with an arsenal of both conventional and nuclear armaments. Weaponry included ICBMs and bombers in numbers that dwarfed Soviet forces. This modernization and expansion of the missile system confronted any potential aggressors with the impossibility of a strategic victory and the certainty of total destruction. It also established a direct connection between national security policy and strategic forces procurement.

The Kennedy administration security strategy, called "flexible response" because it expanded the options for fighting the communist threat, rested on three cornerstones. Along with a dramatic increase in the nation's military, Kennedy increased economic and military assistance to the developing world. The Agency for International Development coordinated foreign aid, while the Alliance for Progress acted as a blueprint for Latin America by promoting massive modernization and development. The most celebrated economic aid program offered by the administration was the Peace Corps, established by executive order in 1961. This volunteer group, consisting mostly of young adults, went into developing nations as teachers, agricultural advisers, and technicians. The Peace Corps involved the implicit assumption that technical expertise rather than anti-communist ideology and military dominance would be the best way to win support in the developing world. The last aspect of flexible response aimed to deter aggression by training Latin American paramilitary forces. The Pentagon established the Jungle Warfare School, which taught Latin American police officers how to infiltrate leftist groups.

Kennedy's desire to assist democracy in Latin America led to a serious blunder. As president-elect, Kennedy learned of a secret CIA plan for the invasion of Cuba by anti-communist refugees who had fled the nation when Fidel Castro took power. A few aides expressed doubts about the viability of the plan, but Kennedy was determined to strike against communism in Cuba. The decision to abandon the bureaucratic NSC may have contributed to the resulting debacle. The NSC, which rarely met, did not handle the decision to invade Cuba. The attack, in April 1961, failed within three days. The exposure of U.S. involvement led to widespread international condemnation and a humiliating loss of prestige in Latin America.

In late 1961, an American U-2 spy plane photographed intermediate-range nuclear missile sites in Cuba. Military officials warned Kennedy that the missiles would soon be operational and could strike cities along the East Coast of the United States. If Kennedy declined to respond to the

presence of Soviet missiles in the Western Hemisphere, Soviet prestige in the Third World would be bolstered and the communists would gain an important bargaining chip for future negotiations on other issues. After rejecting an air strike to destroy the missiles because the Soviets were likely to respond in a manner that would trigger a general nuclear war, Kennedy imposed a naval blockade of Cuba. The Soviets eventually backed down and removed the missiles, but not before the U.S. and the U.S.S.R. came close to war.

The possibility of nuclear war, brought home by the Cuban missile crisis, led to a softening of Cold War attitudes and a new emphasis on cooperation. The White House and Kremlin agreed to the installation of a "hot line" to establish instantaneous communication between the two superpowers. In 1963, the thaw in relations led to the signing of the Nuclear Test Ban Treaty, which halted atmospheric and underwater nuclear testing.

The Kennedy administration came into office with a determination to continue the aggressive Cold War policies of the past. Although it focused on aid to the developing world, little changed in regard to basic national security policy until 1962. The Cuban missile crisis brought the U.S. to the brink of a possible nuclear war and forced a reexamination of American attitudes toward the Soviet Union and the Cold War.

#### ■ FURTHER READING:

##### BOOKS:

- Ball, Desmond. *Politics and Force Levels: The Strategic Missile Program of the Kennedy Administration*. Lexington: University Press of Kentucky, 1988.
- Boll, Michael M. *National Security Planning Roosevelt Through Reagan*. Lexington: University Press of Kentucky, 1988.
- Crabb, Cecil V., and Kevin V. Mulcahy. *American National Security: A Presidential Perspective*. Pacific Grove, CA: Brooks/Cole, 1991.

##### ELECTRONIC:

- White House. "History of the National Security Council, 1947–1997." <<http://www.whitehouse.gov/nsc/history.html>> (April 25, 2003).

##### SEE ALSO

- Ballistic Missiles*  
*Bay of Pigs*  
*Berlin Wall*  
*Cold War (1950–1972)*  
*Cuban Missile Crisis*  
*DIA (Defense Intelligence Agency)*  
*Executive Orders and Presidential Directives*  
*National Security Strategy, United States*  
*NSC (National Security Council)*  
*NSC (National Security Council), History*  
*U-2 Spy Plane*



Rescue workers pull an injured man from the ruins of a neighboring building after a powerful blast detonated next to the U.S. Embassy in Nairobi, Kenya, in 1998. Islamist al-Qaeda members were blamed for the explosion, which killed over 200 people and injured over 1,600. AP/WIDE WORLD PHOTOS.

## Kenya, Bombing of United States Embassy

■ MICHAEL VAN DYKE

At approximately 10:30 on the morning of August 7, 1998, a yellow van approached the United States Embassy in Nairobi, Kenya. When the vehicle stopped, one of the passengers exited and threw a grenade-like device at the gate-guard. The guard fled while the van went through the gate and proceeded to the underground parking garage. Moments later, an explosion ripped through the embassy, also demolishing the nearby Ufundi Coop House and the 17-story Cooperative Bank. A secretarial college was also severely damaged. Two hundred and fourteen persons were killed in the bombing, including twelve American citizens, and more than four thousand were injured. A near-simultaneous bombing of the U.S. Embassy in Dar es Salaam, Tanzania, killed eleven more people.

Within days, the man who had thrown the grenade-like device was captured and identified as Mohamed Rashed Daoud al-Owhali. Al-Owhali had been injured in the grenade explosion and had gone to a local hospital for treatment. Under questioning, al-Owhali revealed that the operation was linked to the Arab-Afghan al-Qaeda

organization run by Saudi financier Osama bin Laden. Al-Owhali claimed to have been trained in several al-Qaeda terrorist camps in Afghanistan, where he had received instruction in explosives, highjacking, and kidnapping. He had also attended conferences where Bin Laden was present, and was aware of a 1996 fatwa (religious ruling), signed by Bin Laden, that urged the killing of Americans worldwide. Al-Owhali also stated that the bombing was supposed to have been a “martyrdom operation,” and that he hadn’t expected to survive it. Soon thereafter, a second suspect was captured and identified as Mohamed Sadiq Odeh. Odeh, a 34-year-old Palestinian engineer, admitted that he had provided technical and logistical support to the bombers. Further investigation showed that Odeh had been a member of al-Qaeda since 1992, and had lived in Kenya since 1996, where he had been in frequent communication with top al-Qaeda commanders. He also was aware of Bin Laden’s 1996 fatwa. Al-Owhali, the first suspect, was a Yemeni national who agreed to speak to authorities if he was guaranteed trial in the United States (“because America is my enemy and Kenya is not”). In his testimony, al-Owhali claimed that the Nairobi embassy had been targeted because it was a lightly guarded, “easy target.” In regard to the timing of the bombing, al-Owhali testified that it had been planned for late Friday morning because observant Muslims would be going to mosques for prayer services at that time.

Within weeks of the bombing, the United States responded with SCUD missile attacks on likely Bin Laden base camps in Afghanistan. Satellites had observed the dispersion of people away from these camps in the days immediately following the August 7 embassy bombings. Combined with the testimony of al-Owhali and Odeh, these observed movements gave the United States evidence to consider al-Qaeda and Osama bin Laden fully responsible for the deadly attacks. By the fourth anniversary of the bombing, the United States had given \$42 million in assistance to Kenya and four of the perpetrators had been convicted and sentenced to life in prison.

## ■ FURTHER READING:

### BOOKS:

- Benjamin, Daniel, and Steven Simon. *The Age of Sacred Terror*. New York: Random House, 2002.
- Gunaratna, Rohan. *Inside Al Qaeda: Global Network of Terror*. New York: Columbia University Press, 2002.
- Kushner, Harvey W., ed. *Essential Readings on Political Terrorism: Analyses of Problems and Prospects for the 21st Century*. Lincoln, Nebraska: Gordian Knot Books, University of Nebraska Press, 2002.

### ELECTRONIC:

The Avalon Project at Yale Law School. "Documents on Terrorism: Criminal Complaint Against Kenya Bombing Suspect Al-Owhali." August 26, 1998. <[http://www.yale.edu/lawweb/avalon/terrorism/t\\_0024.htm](http://www.yale.edu/lawweb/avalon/terrorism/t_0024.htm)> (December 13, 2002).

### SEE ALSO

*Clinton Administration (1993–2001), United States National Security Policy*  
*Enduring Freedom, Operation Interrogation*  
*Satellites, Spy*  
*September 11 Terrorist Attacks on the United States*  
*Terrorist and Para-State Organizations*  
*Terrorist Organization List, United States*  
*United States, Counter-terrorism Policy*

## Keyhole Satellites.

SEE *Satellites, Spy*.

## KGB (*Komitet Gosudarstvennoi Bezopasnosti*, USSR Committee of State Security)

■ K. LEE LERNER

The KGB (*Komitet Gosudarstvennoi Bezopasnosti* or Committee of State Security) was the preeminent Soviet intelligence agency and Soviet equivalent of the American CIA.

The KGB was the primary organization for intelligence and counterintelligence matters during the later Soviet period. Although the NKVD was tasked with internal security, the KGB role in political security and counterintelligence was so broad that its operations often touched on internal security matters. For example, in 1957, Soviet border guards were placed under KGB supervision.

The KGB and Western intelligence services played a continual deadly game of "cat and mouse" (both as pursuers and the pursued) throughout the Cold War, with some of the most intense activity centered on Berlin (e.g., Operation Gold and the Berlin tunnel episode). In 1967, Yuri Andropov, then head of KGB and later Soviet premier, described the role of the KGB and other state security bodies as "a bitter and stubborn battle on all fronts, economic, political, and ideological."

**Origin and formation of the KGB.** The first Soviet state security organization, the Cheka (aka, Vecheka or All-Russian Extraordinary Commission for Combating Counter-revolution and Sabotage) was created by the new Soviet leaders almost immediately following the November revolution in 1917. In 1922, the State Political Directorate (GPU) succeeded the Cheka and was then placed under the control of the NKVD (People's Commissariat of Internal Affairs).

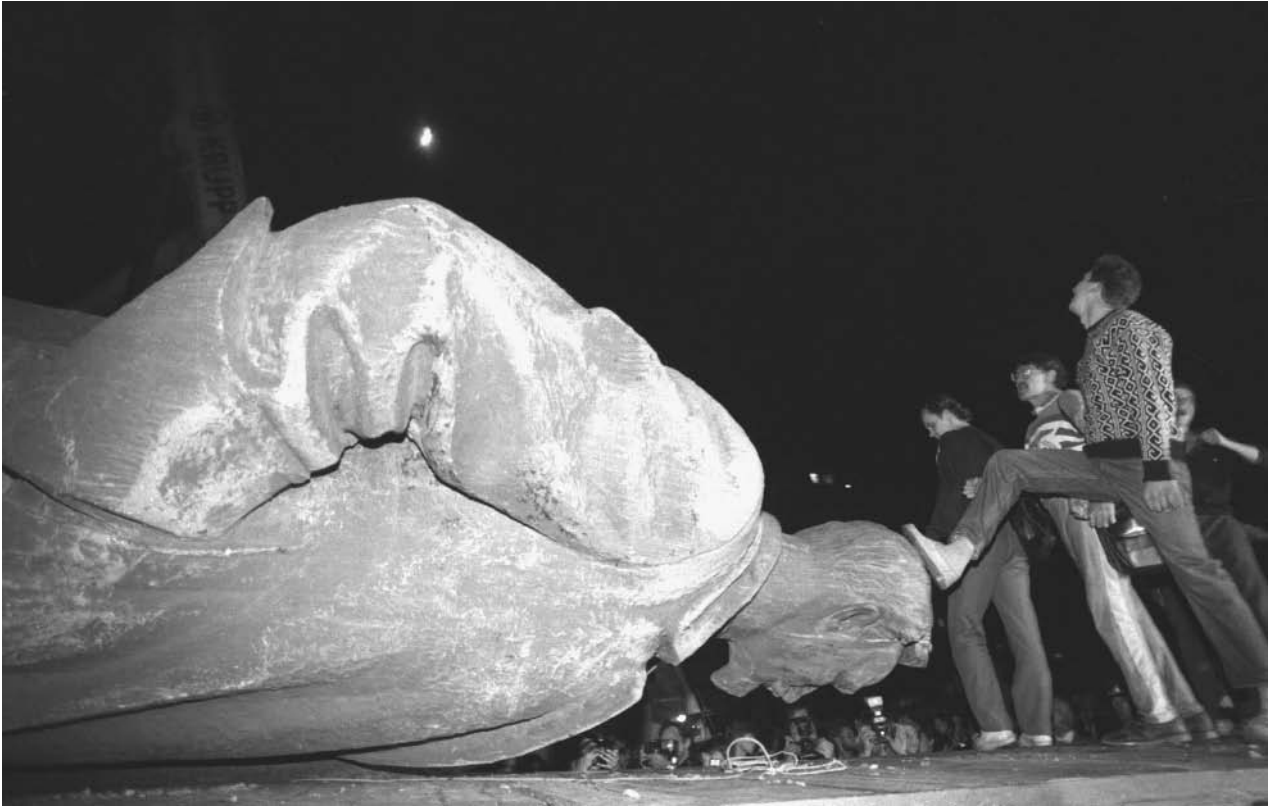
When the Union of Soviet Socialist Republics was formally created the next year, the GPU became the OGPU (Unified State Political Directorate) and was made an independent directorate (disassociated from the NKVD) of the Soviet Council of People's Commissars. In the political infighting and turmoil of the early 1930s in the Soviet Union, the OGPU was renamed the GUGB (Chief Directorate of State Security) and simultaneously placed under the control of the also reformed All-Union NKVD.

This fusion of state security and intelligence functions produced powerful influence embodied in a string of leaders that included G. G. Yagoda, N. I. Yezhov (1936), and Lavrentii Beria (1938).

In 1941, during World War II, the GUGB was split from the NKVD and granted equal status as the NKGB. The first NKGB director, V. N. Merkulov, had worked directly with Beria and followed similar brutal methodologies. The NKGB was tasked with conducting both external espionage and counter-espionage activities as well as guaranteeing Communist Party rule by suppressing counter-revolutionary organizations.

As the Nazi invasion pushed deeper into Russia, the NKGB was once again briefly fused with NKVD under its old title as the GUGB to streamline efforts to coordinate an effective defense against the Nazi forces. As the front stabilized and the Soviets began to push the Germans back, the GUGB was once again given independent status as the NKGB.

Derived from special sections of the NKVD Army (NKO) and Navy (NKVMF), a powerful new element,



Russians step on the head of the statue of the founder of the KGB, Felix Edmundovich Dzerzhinsky. The statue, which had long stood in front of KGB headquarters in Moscow, was toppled in 1991 as thousands of Muscovites watched. AP/WIDE WORLD PHOTOS.

SMERSH (*SMERt SHpionam* or “Death to Spies”) became a forerunner to KGB assassination teams. In 1940, Leon Trotsky was assassinated in Mexico City by SMERSH. Trotsky had long been a rival of Soviet dictator Josef Stalin, who recognized that Trotsky’s role in launching the Bolshevik takeover of Russia alongside V. I. Lenin gave him much greater revolutionary legitimacy. SMERSH agents tracked Trotsky for more than a decade before the assassination.

Following World War II, the Soviet government renamed the People’s Commissariats as ministries and the NKVD became the MVD and the NKGB became the MGB. In March, 1953, the day after Stalin died, Beria united the MGB and MVD into one organization (retaining the title MVD). After Beria’s trial and execution in 1954, espionage activities were assigned to a reconstituted unit designated as the KGB and placed under the direction of the Soviet Council of Ministers. In 1978, the KGB chairman was assured a place on the Soviet Council of Ministers.

As part of his attempted reforms of the Soviet Union (e.g., *glasnost*), the last Soviet premier, Mikhail Gorbachev also attempted to reform the KGB before it was dissolved in 1991 but these attempts were met with resistance within the KGB hierarchy and eventually created tension significant to the collapse of the Soviet Union. The fate of

the KGB was sealed when its leader, Colonel General Vladimir Kryuchkov, ordered KGB agents to participate in the failed August, 1991, coup attempt against Mikhail Gorbachev. KGB-directed forces surrounded Gorbachev’s Crimean dacha (house) for three tense days before the coup collapsed.

The Soviet Union collapsed and splintered in 1991. The KGB was dissolved and the *Federal’naya Sluzhba Bezopasnosti*, or Federal Security Service (FSB), Russian Federal Counterintelligence Service (FSK), and Foreign Intelligence Service (SVR) were formed (from resources that included some former KGB elements) to serve the intelligence needs of the new Russian Federation.

**KGB tactics.** KGB operatives were masters at tactics ranging from disinformation (in Russian, *dezinformatsiya*) to assassination. As did their Western counterparts, KGB operatives also employed technology specifically designed for espionage operations. KGB agents employed a range of weapons, including exotic devices like poison pens that fired hydrocyanic acid gas or pellets of ricin. Another celebrated example involved the KGB development of the lipstick pistol, or “kiss of death.” Created by KGB scientists, the lipstick pistol contained a 4.5-mm single-shot pistol encased in rubber and disguised as a tube of lipstick.

The deadly poison ricin came to widespread public attention in 1978, when it was used during the KGB assassination of Bulgarian dissenter Georgi Markov in the United Kingdom. Markov, a BBC broadcaster, died several days after being jabbed by an umbrella at a bridge in London. The poison-tipped umbrella injector was designed by KGB scientists.

KGB operatives used disinformation not only directly against Western governments, but also against governments not following pro-Soviet policies. For example, KGB operatives used disinformation tactics in attempts to destabilize Egyptian president Anwar Sadat for his increasingly pro-Western policies by issuing false statements and writing attributed to Islamist fundamentalists. The disinformation not only contributed to the assassination of Sadat, but also helped fuel Islamist terrorism.

To avoid direct conflict with the U.S., the KGB funded subversive groups and domestic terrorists within the United States (e.g., the Weathermen, a 1960s radical group) through intermediaries such as Cuba.

**Spy vs. spy.** As did their Western intelligence counterparts, KGB officers continually attempted to recruit agents and plant moles in Western intelligence organizations. The KGB's success in this effort was unparalleled, the most infamous success coming with the compromise of British intelligence by the Cambridge University spy ring and mole Kim Philby.

KGB methods of suppression of moles and traitors could be brutal. According to one eyewitness account, when KGB officers discovered a fellow officer had provided information to the CIA, he was thrown feet first into a roaring furnace while his colleagues watched.

The most well known mole for Western intelligence operating within the KGB was Colonel Oleg Penkovsky. Penkovsky initially served the Soviet regime faithfully, but when he became disillusioned with communism and the Soviet leadership, Penkovsky ultimately offered his services to British intelligence. United States President John F. Kennedy used information provided by Penkovsky during the Cuban Missile Crisis. The KGB subsequently arrested Penkovsky. After being convicted of treason, Penkovsky was executed.

**The Legacy of the KGB.** Since the fall of the Soviet Union and the dissolution of the KGB, access to secret archives and testimony of former KGB officers and agents has exposed several double agents. The extent of the Walker family espionage activities became apparent, and specific sensitive U.S. Navy and National Security Agency documents were discovered in the KGB archives.

In 1994, long-time CIA veteran Aldrich Ames was discovered to be a KGB mole. The information he sold to the KGB included the names of Russian double agents and

operatives working for the U.S. within the Soviet intelligence community, ultimately leading to their capture, imprisonment, or execution by Soviet authorities.

In 2001, FBI agent Robert Philip Hanssen was arrested for conspiracy to commit espionage. Hanssen eventually pled guilty to charges that he had spied for the KGB.

Although the predominant sentiment in contemporary Russia is one of relief from fear of the KGB, some express the sentiment that the once omnipresent intelligence-gathering entity was so powerful and invasive that it minimized the commission of ordinary crimes, which now plague Russia.

Some of the bizarre disinformation created by the KGB has become a source of urban legends occasionally regurgitated by ill-informed or profoundly anti-U.S. critics. For example, documents in the KGB archives provide evidence that operatives mounted a disinformation campaign laden with pseudo-scientific "proofs" that the United States had deliberately created the AIDS virus in the laboratory to use as a biological weapon.

The KGB mounted a major disinformation campaign during the Korean War that resulted in lasting influences on North Korean and Western relations. KGB operatives disseminated information that accused U.S.-led United Nations forces of using biological and chemical warfare against North Korean civilians, information that is still propagated by the North Korean government and so continues to poison public opinion against the U.S. and other Western powers.

#### ■ FURTHER READING:

##### BOOKS:

- Bittmann, Ladislav. *The KGB and Soviet Disinformation*. Washington: Pergamon-Brassey's International Defense Publishers, 1985.
- Kessler, Ronald. *Moscow Station: How the KGB Penetrated the American Embassy*. New York: Scribner's, 1989.
- Mitrokhin, Vasily, ed. *KGB Lexicon: The Soviet Intelligence Officer's Handbook*. London: Frank Cass, 2002.

##### PERIODICALS:

- Gordievsky, Oleg. "The KGB Archives." *Intelligence and National Security* 6, no. 1 (Jan. 1991): 7–14.
- Waller, Michael J. "State within a State: The KGB and its Successors" *Perspective* IV, no. 4 (1994).

##### OTHER:

- Romerstein, Herbert. "Disinformation as a KGB Weapon in the Cold War." Prepared for a Conference on Germany and Intelligence Organizations: The Last Fifty Years in Review, sponsored by Akademie fur Politische Bildung Tutzing, June 18–20, 1999.

##### SEE ALSO

- Ames (Aldrich H.) Espionage Case*

*Assassination*  
*Assassination Weapons, Mechanical*  
*Berlin Tunnel*  
*Biochemical Assassination Weapons*  
*Cambridge University Spy Ring*  
*Cameras*  
*Cameras, Miniature*  
*CIA (United States Central Intelligence Agency)*  
*CIA, Formation and History*  
*Cold War (1945–1950), The Start of the Atomic Age*  
*Cold War (1950–1972)*  
*Cold War (1972–1989): The Collapse of the Soviet Union*  
*Concealment Devices*  
*Crime Prevention, Intelligence Agencies*  
*Cuba, Intelligence and Security*  
*Czech Republic, Intelligence and Security*  
*Dirty Tricks*  
*Disinformation*  
*Document Forgery*  
*Double Agents*  
*Hanssen (Robert) Espionage Case*  
*Intelligence Agent*  
*MI5 (British Security Service)*  
*MI6 (British Secret Intelligence Service)*  
*Propaganda, Uses and Psychology*  
*Rosenberg (Ethel and Julius) Espionage Case*  
*Soviet Union (USSR), Intelligence and security*  
*Stasi*  
*Ukraine, Intelligence and Security*  
*Venona*  
*Walker Family Spy Ring*

## Khobar Towers Bombing Incident

■ STEPHANIE WATSON

On June 25, 1996, a truck laden with explosives ignited in front of the Khobar Towers apartment building in Dhahran, Saudi Arabia. The resulting explosion killed 19 American servicemen and wounded hundreds more. It was the second terrorist attack in that country within a year.

In the early 1990s, a fundamentalist Islamist movement was gaining fervor in Saudi Arabia, and its leaders were enraged over the expansion of American and Western influence in that country. Much of their anger was directed at United States military personnel who had established a presence in Saudi Arabia following the 1991 Persian Gulf War. In November 1995, a group of radical Sunni Muslims expressed their rage by setting off a bomb at a Saudi Arabian National Guard facility in the capital city of Riyadh, killing five Americans. The Saudi government in May of the next year executed four of the men involved in the bombing. Following the attack, U.S. intelligence officials uncovered additional threats against American military personnel in Saudi Arabia, but no specific information that would lead them to believe another attack was imminent.

In 1996 more than 3,000 U.S. service personnel were living in the Khobar Towers apartment complex in the port city of Dhahran. On the night of June 25, guards on the roof of the complex were alerted when they noticed two men running from a truck parked near one of the buildings. They acted quickly, but could do nothing to stop the massive explosion that followed. The truck, which was loaded with at least 5,000 pounds of plastic explosives, (larger than the bomb that destroyed the Alfred P. Murrah Federal building in Oklahoma City the previous year) set off an explosion that tore off the northeast side of Building 131, killing 19 Americans and wounding approximately 500 Americans and Saudis.

After the attack, President William J. Clinton announced a “declaration on terrorism,” and called upon other world leaders to join in the fight against international terrorists. The Secretary of Defense appointed a task force to investigate the incident, and began implementing measures to protect against future attacks.

**The investigation.** Soon after the attack, a local wing of the Lebanon-based militant group Hezbollah claimed responsibility. Terrorism experts extrapolated that Iran also played a role in the bombing, in part because it backs the Hezbollah. Iranian officials denied playing a role in the attack, and claimed that the terrorists were not in their country. Saudi officials asserted that the bombing was the work of Saudi dissidents who were aided by Iran. Although the Saudis rounded up several suspects, they were reluctant to share information with the CIA and FBI, and were unwilling to provide the Americans with access to the detainees. In March 1997, a Saudi citizen named Hani Abdel Rahim Hussein Al-Sayegh was arrested in Canada. American authorities later claimed he gave the signal for the bombing.

Following a nearly five-year investigation, on June 21, 2001, a federal grand jury in Virginia indicted thirteen Saudis and a Lebanese man on charges of murder and conspiracy in the Khobar Towers bombing. Nine of the men were charged with forty-six criminal counts, ranging from conspiracy to kill Americans and employees of the United States, to bombing and murder. The other five men were charged with five counts each. According to the indictment, all fourteen men were members of Hezbollah, working on orders from Iranian government officials to disrupt the American military presence in Saudi Arabia. According to the Saudi government, many of the named individuals were already in custody at the time of the indictment.

### ■ FURTHER READING:

#### BOOKS:

Ferguson, Amanda, and Nancy L. Stair. *The Attack on U.S. Servicemen at Khobar Towers in Saudi Arabia on June 25, 1996*. New York: Rosen Publishing Group, 2003.



A crater 35 feet deep and 85 feet wide was made by a truck bomb exploded at the Khobar Towers in Dhahran, Saudi Arabia. The bomb killed 19 American servicemen and wounded hundreds more. AP/WIDE WORLD PHOTOS.

#### PERIODICALS:

Duffy, Brian. "Terror in the Gulf: Bombs in the Desert" *U.S. News & World Report*. July 8, 1996: 28–32.

#### SEE ALSO

*Clinton Administration (1993–2001), United States National Security Policy*  
*DOD (United States Department of Defense)*  
*FBI (United States Federal Bureau of Investigation)*  
*Iran, Intelligence and Security*  
*Persian Gulf War*  
*Saudi Arabia, Intelligence and Security*  
*Terrorist Threat Integration Center*  
*USS Cole*

### Kinetic Weapons.

SEE *Strategic Defense Initiative and National Missile Defense*.

### Kiss of Death.

SEE *Assassination Weapons, Mechanical*.

## Knives

■ JUDSON KNIGHT

Knives come in all shapes and sizes, but for many of the purposes for which an undercover operative might need one, small is preferred; hence, the plethora of diminutive edge weapons available to persons working covert operations for a well-supplied organization such as the Central Intelligence Agency (CIA). Knives may be used for escape and related applications such as lock-picking, or—more infamously—to inflict personal harm. For the latter application, where assassination is the intent, concealment is key, and small daggers (a smaller instrument, made purely for stabbing) are favored. Other knives are made for close combat, in which case a longer blade offers an advantage.

**Small knives for concealment.** At the extremely small end are thumb knives, lapel daggers, coin knives, and the like. Developed by the British in World War II, the coin knife looks like an ordinary piece of pocket change, which makes it easy for a prisoner to keep it on his person, even after being searched. The blade itself is crescent-shaped, and attaches to the back by a small hasp so that it can



A butterfly knife carried by German pilots in World War II helped downed pilots and paratroopers cut through parachute lines. AP/WIDE WORLD PHOTOS.

rotate outward. It is too blunt to be used for inflicting bodily harm, but can be useful in escape. The inside of the blade is much sharper, after the manner of a cigar cutter, and was sometimes used to slice through the tire stems on German vehicles during the war. The British favored their one-pence piece, though any large coin would serve the purpose.

A similar concept is the ring knife, whose blade is much sharper than that of the coin knife, and not retractable. To conceal its purpose, users hide the curved blade on the inside of the hand until it is needed, at which point the ring can be turned around and used. Lapel daggers, also used widely by the Allies and Resistance in World War II, resemble thumb knives. (The latter are discussed elsewhere, in the context of assassination weapons.) Very sharp and short, the lapel dagger often had a hole at one end, through which passed a loop to attach it to the forefinger so as to ensure greater control when using it. Originally these weapons really were concealed in lapels, but after the Germans became aware of this practice, agents found other places to hide them, including in the lining of their clothes. Some hid them in their socks after the style of the kilted Scottish warriors, whose *shen du* had been the model for the lapel dagger.

**Long knives for power.** Knives and daggers have been concealed in belts (that is, on the inside of the belt and

parallel to it), in belt buckles, and even in the plastic arms of eyeglasses. But when the user is going into a situation of open combat, and concealment is not necessary, a large knife is desirable. An example is the throwing knife, which looks like an elongated spear point (though with the flanges rounded off) along with about six inches of the “spear” itself as a grip. It is very thin, which makes it easy to throw, but in order to be effective, it must be thrown with both accuracy and power, and throwing must be followed by one or more thrusts at close quarters.

Most formidable-looking of all is the Fairbairn-Sykes fighting knife, developed in World War II by two British officers, W. E. Fairbairn and E. A. Sykes. Based on knowledge gained from their experience in close combat while serving with the Shanghai police, the knife would quickly dispatch a victim by striking at his vital organs. Its blade was long, but the handle was nearly as lengthy, so as to ensure great control on the part of the user. First produced in 1941, it was readily adopted by the Allies. British commandoes carried it on raids into Norway, and the United States Office of Strategic Services (OSS), which employed Fairbairn as an instructor, developed its own version. Revised over the years, the knife remained in production through the 1990s.

#### ■ FURTHER READING:

##### BOOKS:

- De Riaz, Yvan A. *The Book of Knives*. New York: Crown, 1981.
- Melton, H. Keith. *The Ultimate Spy Book*. New York: DK Publishing, 1996.
- Minnery, John. *CIA Catalog of Clandestine Weapons, Tools, and Gadgets*. Boulder, CO: Paladin Press, 1990.
- Stephens, Frederick John, and Michael Boxall. *Fighting Knives: An Illustrated Guide to Fighting Knives and Military Survival Weapons of the World*. New York: Arco, 1980.

##### SEE ALSO

*Assassination Weapons, Mechanical*

## Korean War

#### ■ JUDSON KNIGHT

Although it is often described as the “forgotten war,” the conflict in Korea cost some 3 million lives over the course of three years, and helped set the tone for the larger Cold War. Both an international and a national conflict, the Korean War demonstrated the strengths and limitations of the United Nations (UN), and established the framework for the policy of containment that would lead the United States into the much longer conflict in Vietnam. Korea also solidified American attitudes toward communism, and





Korean war spy John T. Downey, freed after 20 years in Chinese prison, when asked in 1973 if he had revealed any secret information answered, "I can say, yes. I revealed about every information I had." ©BETTMANN/CORBIS.

reaction to events there served to influence both the rise of Senator Joseph McCarthy and the fear of communist "brainwashing." As much a war of intelligence as of arms, Korea saw the birth of the modern U.S. signals intelligence framework as the Armed Forces Security Agency (AFSA) gave way to the National Security Agency (NSA). In the end, an allied force of South Korean, American, British, Australian, and Turkish troops frustrated the aspirations of the North Korean Communist government, aided by the People's Republic of China, to control the Korean peninsula. The truce in 1953 established an uneasy framework—not quite war, not quite peace—that nevertheless remains in place half a century later.

## Background

The roots of the Korean War, like those of the Vietnam conflict, lay in World War II. Soon after 1945, the British

and American alliance with the Soviet Union broke down in Europe, and the Korean hostilities brought the end of this partnership in Asia as well. The Soviets had fought World War II entirely on their western front, and only entered the Pacific war on a last minute bid for territory. Years earlier, the little-known tank battle between Soviet and Japanese forces at Nomonhan in August 1939, had discouraged Japan from any hope that a war with the Soviets would yield easy victory. Therefore, when Adolf Hitler invaded the Soviet Union in June 1941, his Japanese allies did not join him in making war on Russia.

Soviet dictator Josef Stalin's lack of participation in the Pacific theatre did not preclude his plans to extend the reach of Soviet Communism into that area. He was aided by an agreement with the United States that the Japanese would surrender to Soviet forces north of the 38th parallel on the Korean peninsula, which enabled him to establish a Communist government in Pyongyang under the

leadership of Kim Il Sung. (Despite North Korean state hagiographers' later attempt to recast their "Great Leader" as a war hero, in fact he had spent the entire war under Stalin's protection, behind Soviet lines.)

By 1947, it had become apparent that Korea, in Japanese hands since 1910, would not easily be reunited under a non-Communist government. Soon another event served to further raise the specter of Communist expansionism in Asia. In October 1949, the victory of Mao Zedong's forces placed the world's largest population under the Communist rule of the People's Republic of China (PRC). Meanwhile, the United States had withdrawn its troops from Korea, and it now petitioned the UN to ensure free elections in Korea. The Soviets had withdrawn their troops as well, but refused to agree to these elections. On June 25, 1950, Kim's armies swept southward to unite the country by force.

An emergency meeting of the UN Security Council resulted in a resolution to stop the North Korean assault. Though the Soviet Union was one of the five permanent Security Council members—along with the United States, United Kingdom, France, and the Republic of China—it had boycotted the meeting in protest of the U.S. effort to block the admission of the PRC. Because of their failure to show up at the Security Council meeting (a mistake they would not again repeat), the Soviets were unable to exercise their veto power against the American call for a "police action" on the Korean peninsula.

Although the Korean conflict is rightly called a war, there was no accompanying declaration by the U.S. Congress; instead, President Harry S. Truman ordered U.S. troops into battle as part of a UN peacekeeping force on June 27, 1950. Four U.S. divisions landed on the Korean peninsula to join the South Korean forces there, but the North Koreans soon drove them all the way to Pusan, at the extreme southeastern end of the peninsula. Soon afterward, however, General Douglas MacArthur abruptly shifted the tide of the war by landing a massive force at Inchon, some 100 miles (160 km) south of the 38th parallel and well behind North Korean lines. He thus, cut the North Korean army in two, and began moving northward, toward what now looked like an easy victory.

As the UN forces moved toward the Yalu River, which separated North Korea from China, Beijing issued a stern warning that it would not look lightly on the presence of a hostile force just across the border. MacArthur, however, remained confident, and at Thanksgiving 1950 promised Americans that their sons would be home for Christmas. This was not to be, as on November 25 the Chinese People's Liberation Army swept across the border with a force of some 180,000 soldiers. By December 15, the allied forces had fallen back below the 38th parallel, and two weeks later, on the last day of 1950, a Chinese-North Korean force numbering half a million troops pushed into South Korea again.

Thanks to relentless bombing by allied forces, the Communist force did not manage to move any further into

South Korean territory, and thus began a lengthy stalemate that would characterize the remainder of the war. American leaders were sharply divided as to the means of resolving the conflict. MacArthur favored an extremely aggressive policy toward China, and proposed a naval blockade combined with bombing of Chinese bases in Manchuria. Truman, however, recognized the danger of such action, which he believed would bring a swift response from the Soviet Union. In the sharply polarized world climate, the price of aggression in Korea would almost certainly be armed conflict with the Soviets, and since they had managed to acquire atomic secrets through spies in the West, the result could very well be nuclear war.

The difference of opinion between MacArthur and Truman characterized that which would come to prevail between hard-line anti-Communists on the one hand, and pragmatists on the other. Overstepping the bounds of his authority as a military leader, MacArthur called on the American people to support his war plans, and for this act of insubordination, Truman relieved him of duty on April 11, 1951. Replaced by General Matthew B. Ridgway, MacArthur returned to the United States a hero, as much for his determination to defeat Communism as for his leadership against the Japanese in World War II. He would become a powerful symbol for the most extreme anti-Communist elements, who soon gained a voice in the Senate under the leadership of McCarthy. Thus began a sort of cold war within the Cold War, a division of the American public that would culminate with the bitter disagreements over the Vietnam War that emerged nearly two decades later.

## Eisenhower and the War's End

Meanwhile, on July 10, 1951, the allied forces began a lengthy series of talks with the Communists. The situation remained unresolved during the 1952 presidential elections, and helped pave the way to victory for Republican presidential candidate Dwight D. Eisenhower. One of the most misunderstood of modern American leaders, Eisenhower was neither a fool nor a hard-liner, and precisely because he had led U.S. forces in Europe during World War II, he recognized the dangers of military adventurism, and tended to be even more of a pragmatist in military matters than Truman had been. Eisenhower, who years later would coin the phrase "military-industrial complex" as he warned against its rise in his farewell presidential address, opposed the Korean War, and vowed to end it.

Winning the presidency with the promise "I shall go to Korea," Eisenhower soon made good on his vow. His policy was the embodiment of Theodore Roosevelt's famous dictum about walking softly and carrying a big stick: though mild on the surface, in private discussions with Chinese leaders he made it clear that he would take aggressive steps, up to and including the use of nuclear weapons, if the talks were not soon brought to resolution. Though fighting resumed briefly in June 1953, in the end Eisenhower's gambit won out, and on July 27, the two

sides signed an armistice. Although the South gained possession of some eastern mountains north of the 38th parallel, the line virtually served as the boundary between North and South Korea.

In keeping with the emerging modern face of warfare, the Korean conflict was as much a battle of propaganda and intelligence as it was one of military forces. Both sides took large numbers of prisoners of war (POWs), which they exchanged at the end of the fighting, and the Communists in particular made heavy use of the propaganda value to be gained from POWs. Eight different POW camps dotted a stretch along the Yalu River, and in these facilities the Communists sought to demoralize their captives by segregating them according to rank, nationality, and even race. They bombarded the POWs on a daily basis with lessons on the superiority of Communism over capitalism, but the purpose of these activities seems to have been harassment rather than an actual effort to win converts.

The experience added a new term to the English language: brainwashing. The term referred to a variety of psychological and sometimes physical techniques intended to obliterate an individual's beliefs and replace them with new ones. Despite fears of brainwashing that spread through American society in the war's aftermath, there was never any conclusive psychological proof that brainwashing as such actually occurred. Some servicemen did make statements favorable to their captors, and others collaborated with the Communists, but these actions were the result either of fatigue under captivity, or of a simple desire for self-preservation.

**Allied signals intelligence.** In the behind-the-scenes dimension of the Korean War, the success of allied efforts in signals intelligence (SIGINT) was much more firmly established than that of the Communists in brainwashing. Continuing their record of achievements established in World War II, British and American cryptanalysts proved highly adept at breaking Chinese ciphers. Of particular significance was the breaking of Chinese one-time pad ciphers, which had been supposedly unbreakable, by American cryptanalysts. This was especially noteworthy in light of criticisms that U.S. intelligence had failed to predict the coming of the war itself.

In fact, the modern U.S. intelligence community had only barely come into existence at the war's outset, and Korea marked a turning point. Before the war, budgets for intelligence operations had been lean, but after the outbreak of hostilities, Washington made a much firmer commitment to its intelligence community. Only three years before the war began, the National Security Act of 1947 had established the Central Intelligence Agency, and NSA had yet to be born. Instead, AFSA coordinated all cryptographic activities, though the leading SIGINT agency for the U.S. forces was the Army Security Agency (ASA).

Whereas AFSA is remembered as an administrative failure, and was further tainted by the discovery that one

of its personnel, William Weisband, had been working for the Soviets since 1934, ASA had a number of notable successes. It cultivated a program of Korean linguists, and used a signal intercept technique from World War I to great effect. This was the ground-return intercept, which used the principle of electric induction to pick up Chinese and North Korean telephone traffic. Also significant was the work of the Air Force Security Service (AFSS), which regularly intercepted information on planned bombing runs and helped allied forces protect their facilities. As for the AFSA, it had been formed to coordinate the SIGINT activities of the military services, but by 1952 Washington had recognized its lack of success in doing so, and in that year a secret memo from Truman established the NSA.

## The Legacy of Korea

Some 37,000 Americans died in Korea, along with smaller casualties among the British, Australian, and Turkish forces. The North Koreans lost half a million soldiers, and the Chinese sustained losses of one million. By far the worst casualties belonged to the South Koreans, who lost 1.3 million civilian and military personnel. Though the war resulted in a stalemate, it preserved South Korean independence, and resulted in the establishment of boundaries that remained in place 50 years later.

The war helped draw sharp lines between the Communist world and the West, and in its immediate aftermath, Americans were confronted with the specter of not one but two Communist superpowers allied against them. The Soviet-Chinese alliance would not hold, however, and by 1969 the two nations had become more hostile toward one another than either was toward the United States.

By gaining what could be construed as a victory in Korea, American leaders came away with the mistaken impression that large commitments of troops was a viable means of containing Communist expansion in small Asian nations. Thus, within a year of the Korean War's end, U.S. forces would become involved in another effort to roll back the Communist tide on the Asian continent, this time much further south, in Vietnam.

As for the two countries whose conflict had drawn the world's attention, the war only solidified the division between them. For many years, South Korea would maintain a strict authoritarian regime that, while liberal in comparison to that of North Korea, was hardly so by modern standards. In the 1980s, however, it would emerge as an economic powerhouse, and as its populace prospered, they began to demand greater political options. In time, their nation would become an example of the relationship between economic and political liberalization.

By contrast, North Korea would serve to exemplify the disastrous consequences of strict totalitarian control in practice. An Orwellian state, it was the virtual kingdom of Kim, which he would pass on—along with the gruesome cult of personality that developed around him—to his son Kim Jong Il upon his death in 1994. Plagued by

famine, unable to sustain even the most basic needs of its populace, North Korea survived on the remittances sent home by citizens living in Japan, and by arms sales to other rogue dictatorships. Its development of missile technology, which it exported to extremist regimes of the Islamic world, would earn it a place, along with Iran and Iraq, on the “axis of evil” described by President George W. Bush in 2002.

#### ■ FURTHER READING:

##### BOOKS:

- Blair, Clay. *The Forgotten War: America in Korea, 1950–1953*. New York: Times Books, 1987.
- Goulden, Joseph C. *Korea, the Untold Story of the War*. New York: Times Books, 1982.
- Hastings, Max. *The Korean War*. New York: Simon and Schuster, 1987.
- Ridgway, Matthew B. *The Korean War: How We Met the Challenge; How All-Out Asian War Was Averted; Why MacArthur Was Dismissed; Why Today's War Objectives Must Be Limited*. Garden City, NY: Doubleday, 1967.
- Stokesbury, James L. *A Short History of the Korean War*. New York: W. Morrow, 1988.
- Toland, John. *In Mortal Combat, Korea, 1950–1953*. New York: Morrow, 1991.
- Tomedi, Rudy. *No Bugles, No Drums: An Oral History of the Korean War*. New York: Wiley, 1993.
- Weintraub, Stanley. *MacArthur's War: Korea and the Undoing of an American Hero*. New York: Free Press, 2000.

##### ELECTRONIC:

- Korean War 50th Anniversary Commemoration. U.S. Department of Defense. <<http://korea50.army.mil/>> (April 12, 2003).
- NSA Korean War 1950–1953 Commemoration. National Security Agency. <<http://www.nsa.gov/korea/>> (April 12, 2003).

##### SEE ALSO

*Army Security Agency*  
*COMINT (Communications Intelligence)*  
*McCarthyism*  
*North Korea, Intelligence and Security*  
*North Korean Nuclear Weapons Programs*  
*NSA (United States National Security Agency)*  
*SIGINT (Signals Intelligence)*  
*South Korea, Intelligence and Security*  
*United Nations Security Council*  
*Vietnam War*  
*World War II*

in 1999, marked the first time the organization actually undertook a large-scale troop mobilization. Sparked by genocidal acts on the part of the Serb-dominated Yugoslavian government against ethnic Albanians, the 78-day operation was launched on March 24, 1999. It proved a success, restoring peace to Kosovo and helping to set in motion events that brought about the downfall of Yugoslavia's president, Slobodan Milosevic, 16 months later. Of perhaps even greater significance, it illustrated NATO's capability to fulfill the peacekeeping mission for which it had been established 50 years earlier.

**Prelude to war.** The symbolic significance of Kosovo loomed large in the worldview of Serbian nationalism. It was there, on June 28, 1389, that Serbian armies had lost to the Ottoman Turks, an event lodged in the Serbian consciousness comparable to Pearl Harbor in that of Americans. When Serbian student Gavrilo Princip shot the visiting Austrian archduke Francis Ferdinand in the Bosnian town of Sarajevo on June 28, 1914—the event that launched Europe into World War I—the choice of date was no accident.

Exactly 75 years later, June 28, 1989, marked a key date in the transition from Yugoslav communism to Serbian nationalism. On the 600th anniversary of the battle, Milosevic—a Communist party leader in the Yugoslav federation—spoke at commemoration ceremonies, where he announced that “After six centuries, we are again engaged in battles and quarrels. They are not armed battles, but this cannot be excluded yet.” This met with a roar of approval from the mostly Serbian crowd.

**Milosevic's wars.** In 1991, Milosevic became president of Serbia, and over the following years conducted campaigns of “ethnic cleansing” (elimination, through killing or forced deportation, of non-Serb populations) against Bosnia and Croatia. These led to the first airstrikes in NATO history, in April 1994, against Bosnian Serbs. Further airstrikes, combined with Croat and Bosnian ground offenses, finally brought Milosevic to the bargaining table, and on November 21, 1995, the Dayton Accords ended the war in Bosnia.

Then, in 1996, the Serb army engaged in its first battles with the newly formed Kosovo Liberation Army (KLA), and over the next three years, hostilities continued to escalate. In retaliation for KLA attacks on four policemen, Serb forces on January 15, 1999, killed 45 ethnic Albanians in the town of Racak. The weeks that followed saw repeated attempts at negotiation by officials of the Clinton administration, as well as NATO, the United Nations, and the international Kosovo Verification Mission. All attempts to settle the crisis failed.

**NATO attack begins.** During this time, U.S. attention was primarily focused on the impeachment trial of President William J. Clinton, but when the Senate acquitted him on February 12, Clinton turned his attention to Kosovo and

## Kosovo, NATO Intervention

#### ■ JUDSON KNIGHT

Operation Allied Force, the NATO (North Atlantic Treaty Organization) action in the Yugoslav province of Kosovo

announced plans to deploy 4,000 U.S. peacekeepers. By mid-March, peace talks in Paris had failed, and on March 20, Westerners began to evacuate the Yugoslav capital of Belgrade.

The air war began on March 24, even as Serb forces continued to wage a ground war against ethnic Albanians. On the first night of bombing, NATO warplanes destroyed some 40 targets. In the wake of the attacks and the Serb reprisals that followed, some 800,000 Kosovar Albanians fled the region.

**Operation Allied Force.** In the weeks that followed, the United States faced a number of diplomatic battles with Russia and China, both of which supported Serbia. Initially, Russian president Boris Yeltsin took a hard-line stance with the West, but a change of special envoys to the Balkans in mid-April signaled an attempt to mend relations. The war spread into Albania with the deployment of 24 Apache attack helicopters and 2,000 troops there on April 4. Two days later, NATO missiles misfired, and hit a neighborhood in the mining town of Aleksinac.

Ironically, it was during the Kosovo war that NATO celebrated its 50th anniversary, in Washington, D.C., on April 22. Meanwhile, the war—both of words and armaments—continued. On May 5, NATO experienced its first casualties when two U.S. soldiers were killed in a non-combat helicopter accident, and on May 8, NATO forces accidentally bombed the Chinese embassy in Belgrade, killing three Chinese personnel. Though the Chinese claimed that the attack was no accident, after several tense days they accepted an apology.

**Conclusion and aftermath.** On May 27, the United Nations war crimes tribunal in The Hague, Netherlands, announced an indictment against Milosevic and four other Yugoslav leaders for war crimes in Kosovo. NATO bombers continued to pound Kosovo, and on June 10, 1999, UN secretary-general Javier Solana announced an end to hostilities. Two days later, in a move that surprised Western forces, Russian troops entered Kosovo to take control of the airport at Pristina.

As the Albanians returned in the wake of the NATO victory, some 200,000 Serbs fled. Though outbreaks of ethnic violence continued—most of them reprisals by empowered Albanian nationalists against Serbs—the presence of NATO troops ensured order. Many members of the UCK, the Albanian insurgent army, joined the official Kosovo Protection Force as U.S.-funded efforts began to rebuild houses for some 300,000 people rendered homeless by the bombing. Kosovo-wide elections in October 2000 placed the moderate Democratic League, led by Ibrahim Rugova, in power.

The Serbs evicted from Kosovo descended on Serbia, where they proved a thorn in Milosevic's side. Joined by frustrated soldiers and their families, they conducted a series of protests against the president, and Milosevic responded by calling for early elections—an act that would

prove his undoing. When he changed the election laws to benefit himself and attempted to falsify the outcome, this proved too much for the Yugoslav people, who ousted him. The newly elected government transferred him to The Hague to stand trial for war crimes in June 2001.

#### ■ FURTHER READING:

##### BOOKS:

Clark, Wesley K. *Waging Modern War: Bosnia, Kosovo, and the Future of Combat*. New York: Public Affairs, 2001.

Judah, Tim. *Kosovo: War and Revenge*. New Haven, CT: Yale University Press, 2000.

Malcolm, Noel. *Kosovo: A Short History*. New York: New York University Press, 1998.

Power, Samantha. *A Problem from Hell: America in the Age of Genocide*. New York: Basic Books, 2002.

##### ELECTRONIC:

A Kosovo Chronology. Frontline: War in Europe. Public Broadcasting System. <<http://www.pbs.org/wgbh/pages/frontline/shows/kosovo/etc/cron.html>> (April 7, 2003).

Focus on Kosovo. Cable News Network. <<http://www.cnn.com/SPECIALS/1998/10/kosovo/>> (April 7, 2003).

NATO and Yugoslavia. Radio Free Europe/Radio Liberty. <<http://www.rferl.org/nca/special/nato-kosovo/>> (April 7, 2003).

##### SEE ALSO

*Clinton Administration (1993–2001), United States National Security Policy*

*Cold War (1972–1989): The Collapse of the Soviet Union*

*European Union*

*NATO (North Atlantic Treaty Organization)*

*Serbia, Intelligence and Security*

*United Nations Security Council*

## Kumpulan Mujahidin Malaysia (KMM)

Kumpulan Mujahidin Malaysia (KMM) favors the overthrow of the Mahathir government and the creation of an Islamic state comprising Malaysia, Indonesia, and the southern Philippines. Malaysian authorities believe that smaller, more violent, extremist groups have split from KMM. Zainon Ismail, a former mujahid in Afghanistan, established KMM in 1995. Nik Adli Nik Abdul Aziz, currently detained under Malaysia's Internal Security Act (ISA), assumed leadership in 1999. Malaysian police assert that three Indonesian extremists, one of whom is in custody, have disseminated militant ideology to the KMM. Malaysia is currently holding alleged members of the KMM and its more extremist wing under the ISA for

activities deemed threatening to Malaysia's national security, including planning to wage a jihad, possession of weaponry, bombings and robberies, the murder of a former state assemblyman, and planning attacks on foreigners, including U.S. citizens. Several of the arrested militants have reportedly undergone military training in Afghanistan, and some fought with the Afghan mujahidin during the war against the former Soviet Union. Others are alleged to have ties to Islamic extremist organizations in Indonesia and the Philippines.

Malaysian police assess the KMM to have 70 to 80 members. The Malaysian press reports that police are currently tracking 200 suspected Muslim militants. KMM is reported to have networks in the Malaysian states of Perak, Johor, Kedah, Selangor, Terengganu, and Kelantan. They also operate in Wilayah Persukutuan, the federal territory comprising Kuala Lumpur. According to press reports, the KMM has ties to radical Indonesian Islamic groups and has sent members to Ambon, Indonesia, to fight against Christians.

#### ■ FURTHER READING:

##### ELECTRONIC:

CDI (Center for Defense Information), Terrorism Project.

CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <<http://www.cdi.org/terrorism/terrorist.cfm>> (April 17, 2003).

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001." Annual Report: On the Record Briefing. May 21, 2002 <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

##### SEE ALSO

*Terrorism, Philosophical and Ideological Origins Terrorist and Para-State Organizations Terrorist Organization List, United States Terrorist Organizations, Freezing of Assets*

## Kurdistan Workers' Party (PKK)

Kurdistan Workers' Party (PKK) was founded in 1974 as a Marxist-Leninist insurgent group primarily composed of Turkish Kurds. The group's goal has been to establish an independent Kurdish state in southeastern Turkey, where the population is predominantly Kurdish. In the early 1990s, the PKK moved beyond rural-based insurgent activities to include urban terrorism. Turkish authorities

captured Chairman Abdullah Ocalan in Kenya in early 1999; the Turkish State Security Court subsequently sentenced him to death. In August 1999, Ocalan announced a "peace initiative," ordering members to refrain from violence and requesting dialogue with Ankara on Kurdish issues. At a PKK Congress in January 2000, members supported Ocalan's initiative and claimed the group now would use only political means to achieve its new goal, improved rights for Kurds in Turkey.

Primary targets have been government security forces in Turkey. The PKK also conducted attacks on Turkish diplomatic and commercial facilities in dozens of Western European cities in 1993 and again in 1995. In an attempt to damage Turkey's tourist industry, the PKK bombed tourist sites and hotels and kidnapped foreign tourists in the early to mid-1990s.

PKK strength is estimated at approximately 4,000 to 5,000 members, most of whom currently are located in northern Iraq. The PKK has thousands of sympathizers in Turkey and Europe. PKK operates in Turkey, Europe, and the Middle East, and they receive safe haven and modest aid from Syria, Iraq, and Iran. Damascus generally upheld its September 2000 antiterror agreement with Ankara, pledging not to support the PKK.

#### ■ FURTHER READING:

##### ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001." Annual Report: On the Record Briefing. May 21, 2002. <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

##### SEE ALSO

*Terrorism, Philosophical and Ideological Origins Terrorist and Para-State Organizations Terrorist Organization List, United States Terrorist Organizations, Freezing of Assets*

## Kuwait Oil Fires, Persian Gulf War

#### ■ LAURIE DUNCAN

When Iraqi troops withdrew from Kuwait at the end of the Persian Gulf War in early 1991, they set fire to more than 600 oil wells and pools of spilled oil in Kuwait, a parting shot that exacted a significant economic toll on the country's lucrative petroleum industry. Connecticut-sized Kuwait



An Iraqi tank rests near a series of oil well fires in northern Kuwait during the 1991 Persian Gulf War. Hundreds of fires burned out of control, casting a pall of toxic smoke over Kuwait before firefighting companies, mostly from the United States, extinguished the last fire months later. AP/WIDE WORLD PHOTOS.

contains about 9 percent of the world's total proven oil reserves, and petroleum revenues account for 95 percent of its export earnings. Ignition of oil well fires also created a serious threat to environmental and human health in the Persian Gulf region. The Kuwait oil fires burned for more than eight months, consuming an estimated five to six million barrels of crude oil and 70 to 100 million cubic meters of natural gas per day. Between late February, when the first fires were ignited, and November 6, when the last fire was extinguished, smoke plumes containing a hazardous mixture of gaseous emissions and particulate matter engulfed a downwind area as large as 150 by 1000 kilometers.

The geography and climate of the Persian Gulf region affected the distribution of the oil well plumes, as well as the severity of their effect on human populations and natural ecosystems. Though Saudi Arabia and Iraq border Kuwait's petroleum fields, the region's strong prevailing northerly winds ensured that relatively tiny Kuwait bore the majority of the fires' ill effects. Uneven heating of the land and sea surfaces created local atmospheric inversions during the summer months that trapped smoke in the lower atmosphere, and occasionally caused the plumes to blanket the Kuwaiti land surface. Violent sandstorms, driven by intense summer winds, mixed sand and dust with the smoke plumes.

Kuwait's most productive petroleum reservoir, the greater Al Burqan field, accounted for the majority of the smoke, and for the greatest amount of incinerated oil. Saddam Hussein's Republican Guard set 365 of Al Burqan's approximately 700 wells on fire, and high subsurface pressures kept the fires burning despite heroic firefighting efforts. The Al Burqan fires also presented the greatest risk to human health because of the field's proximity to Kuwait City and the coastal towns where most of Kuwait's approximately two million inhabitants reside.

In general, smoke produced by burning unrefined petroleum contains a mixture of gases and particulate matter including carbon dioxide (CO<sub>2</sub>), carbon monoxide (CO), sulfur dioxide (SO<sub>2</sub>), nitrogen oxides (NO<sub>x</sub>), volatile organics (VOCs), polycyclic aromatic hydrocarbons (PAHs), hydrogen sulfide (H<sub>2</sub>S), acidic aerosols, and soot. (Soot is composed of solid particles embedded in tar.) Non-toxic carbon dioxide accounted for approximately 96 percent of the relatively clean-burning Kuwaiti crude oil smoke. The other chemical elements and compounds in oil well smoke, however, can be toxic, carcinogenic (cancer-causing), and otherwise hazardous to human health, as well as ecologically and climatically disruptive in relatively small concentrations. Airborne measurements above the Al Burqan fires in May and June 1991 found that particulate matter

and gases made up equal parts of the fires' non-carbonaceous emissions. The Al Burqan wells tap Mesozoic-age limestone, dolomite, and sandstone layers containing high-grade crude oil and salt deposits, geologic factors that account for the fairly low concentrations of toxic emissions, and for the presence of salt crystals in the smoke plumes.

Considering the dramatic appearance and scale of the Kuwait oil fires—satellite and space shuttle images showed the plumes extending across the Arabian Peninsula and Persian Gulf, and the smoke blocked the sunlight from large areas for weeks at time—the environmental and human health effects of the fires were much less significant than expected. The largest and longest-burning fires, like those at the Al Burqan field, burned crude oil with low concentrations of potentially harmful impurities, and the “dirtiest” fires, typically pools of crude oil at the surface, were quickly extinguished. Atmospheric inversions kept the plumes close to the land surface where rain droplets and wind-blown dust particles could quickly cleanse harmful particulate matter, organic compounds, and heavy metals from the atmosphere. In fact, numerous studies found that concentrations of most harmful airborne chemicals like VOCs, PAHs, and heavy metals were lower in Kuwait City and at American military bases just miles from the fires than in major cities in the United States. Concentrations were also below levels recommended by American health and industrial regulators. The smoke did contain high levels of particulate matter that may have caused some of the respiratory problems that Kuwaiti residents and Gulf War soldiers reported as symptoms of so-called “Gulf War syndrome.” Fears that the plumes would inject soot and sulfur dioxide into the upper atmosphere and cause global cooling or widespread acid rain also did not materialize.

Kuwait has largely recovered from the socio-economic, environmental, and public health effects of the 1991 oil fires. However, the fires did leave a legacy of more subtle impacts, including long-term environmental damage and chronic human disease. Damaged wells have leaked large amounts of oil into pools on the land surface that threaten fragile desert ecosystems and present a human safety hazard. Furthermore, the Iraqi army set a precedent during the 1991 Gulf War by introducing oil fire ignition as a military tactic. Military forces and threatened nations may face the specter of oil well fires in future armed conflicts in the Middle East and other petroleum-rich regions.

#### ■ FURTHER READING:

##### ELECTRONIC:

Energy Information Administration, U.S. Department of Energy. “Country Analysis Briefs: Kuwait.” August 17, 2002. <<http://www.eia.doe.gov/emeu/cabs/kuwait.html>>(January 4, 2003).

National Defense Research Institute. “A Review of the Scientific Literature as it Pertains to Gulf War Illnesses. Volume 6. Oil Well Fires.” Dalia M. Spektor, Editor. Rand. 1998. <<http://www.gulflink.osd.mil/library/rowl/#contents>>(January 4, 2003).

Public Broadcasting Service. “Last Battle of the Gulf War: Oil-Well Fire Smoke.” Frontline online. 1998. <<http://www.pbs.org/wgbh/pages/frontline/shows/syndrome/analysis/oilwell.html>> (January 4, 2003).

Rove.To. “457 Shuttle Images of Kuwait.” Images from NASA. 1998. <<http://rove.to/kuwait/>>(January 4, 2003).

##### SEE ALSO

*Air Plume and Chemical Analysis  
Environmental Issues Impact on Security  
Natural Resources and National Security*





## Language Training and Skills

■ JUDSON KNIGHT

Language skills are critical to the performance of intelligence, diplomatic, and military duties of many types, both inside the United States and overseas. In this regard, the historic world dominance of English-speaking nations—first the British Empire in the nineteenth century, then the United States in the twentieth and twenty-first centuries—has proven a mixed blessing. On the one hand, the fact that much of the world speaks English offers many advantages, but on the other hand, this fact has kept Americans from learning foreign languages to the extent to which Europeans or other foreign nationals have accomplished the task.

**The need for foreign language skills.** Foreign language skills play a significant role in work for the State Department or its international information programs. These are also vital to HUMINT and SIGINT (human and signals intelligence respectively) work ranging from undercover operations to analysis of raw data captured by eavesdropping. Likewise, military organizations—particularly elite groups such as Delta Force or the Navy SEALs—often look for personnel with a good working knowledge of a language or languages.

In many cases, particularly military or intelligence work, knowledge of obscure languages is likely to be in demand. A diplomat stationed in a West African country, for instance, may speak French to most contacts in the capital city, but intelligence or military operations are likely to take personnel deep into the hinterlands or the underbelly of urban society, where only local languages or dialects are spoken. For example, during the U.S. military effort in Afghanistan in 2001 and thereafter, proficiency in Pashto, Dari, Tajik, and Farsi, the dominant languages in that country, was greatly in demand.

**High demand, small supply.** Coupled with heavy demand is a slim supply of available workers trained in multiple languages. Whereas students in many other countries are required to study English from elementary school onward, few American students are compelled to take more than a few years' worth of a language in high school or college.

Of the languages offered to American students, almost all are Western European tongues. French and Spanish dominate the foreign-language programs in U.S. high schools, and at least these are good starting places for students who hope to work overseas; the vast colonial reach of the Spanish in the sixteenth century, and of the French thereafter, created a world in which millions of Latin Americans speak Spanish, while French is spoken throughout much of Africa, Asia, the Pacific, and selected parts of the New World.

The other languages offered in high schools are not as likely to prove useful to intelligence or military personnel. German, despite its great significance in intellectual history, is seldom useful as an international *lingua franca* because Germany united too late (1870) to develop a significant colonial empire. Only in Central and Eastern Europe is German widely spoken. Latin, the other major language offered in most high schools, is useful as a key to studying the Romance languages (Italian, French, Spanish, Portuguese) derived from it—but there have not been any indigenous Latin-speaking populations for many centuries.

Colleges offer a somewhat broader program, with the other Romance languages, as well as perhaps Russian and even a language or two outside the Indo-European family—Japanese, for instance. The higher a language is on the scale of obscurity, however, the lower (by a great degree) the number of students engaged in its study. According to a 1998 Modern Language Association study, a relatively high number of American college students—25,000—were studying Russian. But Farsi, which is an Indo-European language widely spoken throughout Iran

and central Asia, had only 600 students nationwide. As for Tajik, common to many forces of the Northern Alliance in Afghanistan, fewer than 10 American students every year were studying it.

**The federal language education system.** The federal government has two major language facilities: the Defense Language Institute Foreign Language Center in Monterey, California, and the Foreign Service Institute School for Language Studies in Arlington, Virginia. Additionally, the Defense Language Institute, or DLI, maintains an English Language Center in San Antonio, Texas, for foreign military and government personnel studying English in the United States.

Languages are tested through the Defense Language Aptitude Battery (DLAB) or the Defense Language Proficiency Test (DLPT). Whereas the latter tests proficiency in a particular language, the first test is for job candidates who do not already know the language in question, or perhaps any language other than English. It simply tests language-learning potential, and the only way to prepare for such a test is to master English grammar and syntax, so as to have a good basis for learning an unfamiliar tongue.

Depending on one's score for the DLAB, a candidate may be allowed to progress to a particular course of study at DLI. Below are examples of languages, categorized according to degree of learning difficulty for a native English-speaker, and the score required in order to qualify for that language program:

Category I (Dutch, French, Italian, Spanish, Portuguese): 85

Category II (German): 90

Category III (Greek, Hebrew, Persian, Polish, Russian, Serbo-Croatian, Slovak, Tagalog, Thai, Turkish, Vietnamese): 95

Category IV (Arabic, Chinese, Japanese, Korean): 100

Another system of grading, used by both the government and the educational system in the United States, grades proficiency on a scale from zero to five. Level two is referred to as minimal working proficiency, allowing an individual to function in daily life. Level three, working proficiency, would qualify a person to work as a doctor, professor, or engineer within a foreign culture. Level five is extremely rare in non-native speakers of a language, and indicates full ability to function on a level equivalent to that of a native speaker.

#### ■ FURTHER READING :

##### PERIODICALS:

Molloy, Thomas. "Why Some In-Country English Language Programs Do Not Work." *DISAM Journal of International Security Assistance Management* 24, no. 4 (summer 2002): 125–130.

Peters, Katherine McIntire. "Lost in Translation." *Government Executive* 34, no. 5 (May 2002): 39–45.

Reppert, Barton. "Training the Tongue-Tied." *Government Executive* 34, no. 4 (April 2002): 66.

##### ELECTRONIC:

Defense Language Institute English Language Center. <<http://www.dlielc.org/>> (April 4, 2003).

Defense Language Institute Foreign Language Center. <<http://pom-www.army.mil/>> (April 4, 2003).

Foreign Service Institute. <<http://www.state.gov/m/fsi/>> (April 4, 2003).

National Foreign Language Center. University of Maryland. <<http://www.nflc.org/>> (April 4, 2003).

##### SEE ALSO

*Delta Force*  
*Department of State, United States*  
*DOD (United States Department of Defense)*  
*Enduring Freedom, Operation*  
*Intelligence Community*

## Laser

#### ■ LARRY GILMAN

"Laser" is an acronym for lightwave amplification by stimulated emission of radiation. Lasers exploit the fact that electrons in atoms' outer orbitals can move between energy levels. Like a marble being shifted up and down a set of stairs, an electron can be raised to a higher energy level by giving it the right amount of energy or can give up a fixed amount of energy when it drops to a lower level. The energy given up when an electron drops to a lower level is emitted as a photon (minimal unit of light); the greater the energy lost by the electron, the shorter the wavelength of the emitted light. If the electrons in a material happen to be undergoing energy shifts corresponding to wavelengths that our eyes can see, the material is seen to "glow."

Laser light is a special type of glow. In some materials, a photon passing near an atom with an outer-orbital electron in a high-energy state can, without being absorbed or deflected, stimulate that electron to drop to a lower energy state. The electron gives up its energy in the form of a photon that is of the same wavelength as the impinging photon, in phase with it, and traveling in the same direction. (To say that two photons are "in phase" means that, if they are considered as waves extended through space, their peaks and troughs are aligned; peak matches peak and trough matches trough.) Such light is termed "coherent." Coherent light is rare in nature because atoms in most light sources (e.g., the Sun) are



U.S. ordnance handlers haul a rack of GBU12 laser guided bombs along the deck of the USS *Theodore Roosevelt* in the Arabian Sea in 2001. AP/WIDE WORLD PHOTOS.

emitting photons at random moments and in random directions, independently of each other. In a laser, however, a chain reaction or domino effect occurs.

The electrons in a sample of some substance, for example, a cylinder of gas or a cylindrical crystal of artificial sapphire, are first fed energy—"pumped" to high energy levels. (Pumping was accomplished in all early lasers by illuminating the laser's working substance with intense light, hence "*lightwave* amplification" in the acronym.) If enough of the atoms in the substance are in the excited state to begin with, a domino effect can begin when one atom emits a photon. This photon impinges on a nearby atom, causing it to release a photon having the same frequency, direction, and phase. These two photons go on to stimulate other atoms, which stimulate others,

and so on. The result is that most of the energy locked up in the excited electrons of the laser's working substance is turned quickly into a burst of coherent light. A substance undergoing this process is said to "lase." The resulting light pulse, which is aligned with the long axis of the sample of lasing substance, can be very intense. Lasers that beam continuously, rather than pulsing, can also be built; the trick is to devise a means of continually re-exciting the electrons in the lasing substance as their energy drains away as laser light.

Laser light has several important characteristics: (1) It forms a tight beam, that is, a beam that spreads only slightly with distance. (2) It can be very bright: it is commonplace for a laser to be brighter than the surface of the sun. (3) As all the photons in a given laser beam are produced by identical electron-orbital changes, they are all of the same frequency. That is, a laser beam is of an extremely pure color. (4) Because laser light is coherent, slight shifts in the frequency of laser light, such as those caused by the Doppler effect, are easy to detect. Also, light from a single laser source can be used to interfere with itself after following different paths to a common destination, allowing the extremely precise measurement of distances by the technique termed interferometry.

Since their invention in the 1950s, lasers have found thousands of applications in manufacturing, communications, medicine, astronomy and the other sciences, and weaponry. A few outstanding military applications of laser technology are as follows:

- **Laser-guided weapons.** The distinctive character of laser light—its coherence, brilliance, and purity of color—enables it to stand out from its surroundings, even during broad daylight. Thus, it is easy for a missile to home in on a target (e.g., tank or building) that has been "painted" or illuminated temporarily by a laser beam. Munitions that guide themselves to laser-painted targets are termed laser-guided weapons. Most of the precision-guided munitions in the U.S. arsenal today are laser-guided.
- **Missile-defense lasers.** Beginning with the Star Wars program proposed by President Ronald Reagan in the early 1980s, several schemes have been proposed for using large lasers to shoot down ballistic missiles. The Stars Wars program proposed orbital laser stations or x-ray lasers pumped by nuclear bombs to shoot down ballistic missiles; these ideas were abandoned as too expensive and, possibly, too susceptible to countermeasures. However, development of less-ambitious laser-defense schemes continues. In 2003 or 2004, the U.S. Air Force hopes to perform the first missile-shootdown tests of its YAL-1A Airborne Laser system, a powerful laser mounted on a modified Boeing 747 jetliner.
- **LIDAR.** LIDAR (light detection and ranging) is analogous to radar (radio detection and ranging), but has capabilities that radar does not. In its simplest form, it measures the distance from a laser transmitter to a

reflective object by measuring how much time it takes for a laser pulse to make the round trip. Doppler LIDAR, like doppler radar, deduces the velocity of the target by measuring the frequency shift of the echo. LIDAR can also measure the *composition* of distant reflectors by sending paired laser beams having different frequencies; differing absorption by the substance reflecting the beams (e.g., smoke particles) reveals information about the chemical composition of the target. LIDAR is used by low-flying stealth aircraft to track terrain ahead of them; unlike conventional radar, LIDAR illuminates a very small area of terrain and so is difficult to detect.

- *Virtual retinal displays.* A virtual retinal display shines low-powered lasers mounted on a headset directly onto the retina of the human eye. The display lasers—one for each primary color—are directed at scanning mirrors that rapidly scan the lasers over the user’s retina. (The eyes’ own movements are tracked in real time and compensated for by a computer.) The scanning occurs so rapidly that the user perceives a solid image, not a moving dot of light. Virtual retinal displays have the advantage that they allow the user to see normally at the same time; the image produced by the virtual retinal display is *superimposed* over whatever else the user happens to be looking at. This can be a boon to pilots, allowing them to receive information from electronic sources without having to look away from their flight environment.

#### ■ FURTHER READING:

##### ELECTRONIC:

“Lasers: Spontaneous and Stimulated Emission.” Kottan Labs. 2001. <<http://www.kottan-labs.bgsu.edu/teaching/workshop2001/chapter4a.pdf>> (April 18, 2003).

“Virtual Retinal Display Technology.” Naval Postgraduate School, Department of Computer Science. September 15, 1999. <[http://www.cs.nps.navy.mil/people/faculty/capps/4473/projects/fiambolis/vrd/vrd\\_full.html#VRDworks](http://www.cs.nps.navy.mil/people/faculty/capps/4473/projects/fiambolis/vrd/vrd_full.html#VRDworks)> (April 18, 2003).

##### SEE ALSO

*Laser Listening Devices*

space. As the window-glass is made to move to and fro by the alternating pressure of incident sound waves, some component of its motion will be toward and away from an observer viewing the glass at any angle except 90° to the direction of vibration. Laser light reflected from the glass toward the operator of the laser listening device will, therefore, be Doppler shifted by a continuously changing amount. By detecting this Doppler shift, the vibrations of the reflecting surface, and thus, of the adjacent air, can be detected. Doppler shift occurs when light (or any other moving wave) is reflected from a moving surface or radiated by a moving source. Laser light reflected when the window is vibrating toward the laser listening device is shifted upward in frequency, while light reflected when the window is vibrating away is shifted downward. Laser listening devices have the drawback that they require line-of-sight access to an appropriate reflector; they have the advantage that they can record conversations from a considerable distance and without access to the monitored space itself ever being needed.

Infrared laser light is used in this application both because (a) infrared laser light is invisible, making naked-eye detection of the eavesdropping device unlikely, and (b) because a laser’s light is all emitted at one frequency, measurement of Doppler shift of the reflected beam is straightforward.

Effective laser listening devices are available from commercial suppliers; more sophisticated versions have long been used by various national security agencies. Embassies and other locations wishing to be secure against laser listening devices can deploy such countermeasures as multi-paned windows, exterior meshes to break up laser light, infrared laser detectors, and noise generators that add random vibrations to those caused by conversation.

#### ■ FURTHER READING:

##### ELECTRONIC:

“Spy Suspect Hanssen Betrayed U.S. Countermeasures.” NewsMax.com. March 6, 2001. <<http://www.newsmax.com/archives/articles/2001/3/5/201418.shtml>> (April 16, 2003).

## Laser Listening Devices

Laser listening devices—sometimes termed laser-bounce listening devices—are remote-eavesdropping systems that do not require the placement of a microphone or bug in the space to be monitored. Instead, they measure changes in light reflected from some surface (usually a window) that is made to vibrate by sound waves in the monitored

## Lashkar-e-Tayyiba (LT) (Army of the Righteous)

The Lashkar-e-Tayyiba (LT) (Army of the Righteous) is the armed wing of the Pakistan-based religious organization, Markaz-ud-Dawa-wal-Irshad (MDI), a Sunni anti-U.S. missionary organization formed in 1989. The LT is led by Abdul Wahid Kashmiri and is one of the three largest and

best-trained groups fighting in Kashmir against India. The LT is not connected to a political party. The United States added the group to the list kept by the Treasury Department's Office of Foreign Asset Control (OFAC), which includes organizations that are believed to support terrorist groups and have assets in U.S. jurisdiction that can be frozen or controlled. The group was banned and its assets were frozen by the Pakistani government in January 2002.

The LT has conducted a number of operations against Indian troops and civilian targets in Kashmir since 1993. The LT claimed responsibility for numerous attacks in 2001, including a January attack on Srinagar airport that killed five Indians along with six militants; an attack on a police station in Srinagar that killed at least eight officers and wounded several others; and an attack in April against Indian border security forces that left at least four dead. The Indian government publicly implicated the LT along with the Jaish-e-Mohammed (JEM) (Army of Mohammed) for an attack on the Indian parliament building.

LT has several hundred members in Azad Kashmir, Pakistan, and in India's southern Kashmir and Doda regions. Almost all LT cadres are non-Kashmiris mostly Pakistanis from madrassas across the country and Afghan veterans of the Afghan wars. During attacks, LT uses assault rifles, light and heavy machine guns, mortars, explosives, and rocket propelled grenades. Based in Muridke (near Lahore) and Muzaffarabad, LT trains its militants in mobile camps across Pakistan-administered Kashmir; prior to the fall of 2001, it also conducted training in Afghanistan.

LT collects donations from the Pakistani community in the Persian Gulf and United Kingdom, Islamic NGOs, and Pakistani and Kashmiri businessmen. They also maintain a website (under the name of its parent organization, Jamaat ud-Daawa), through which it solicits funds and provides information on the group's activities. The amount of LT funding is unknown. The LT maintains ties to religious military groups around the world, from the Philippines to the Middle East and Chechnya, through the MDI fraternal network. In anticipation of asset seizures by the Pakistani government, the LT withdrew funds from bank accounts and invested in legal businesses, such as commodity trading, real estate, and production of consumer goods.

## ■ FURTHER READING:

### ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001. Annual Report: On the Record Briefing. May 21, 2002. <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

### SEE ALSO

*Terrorism, Philosophical and Ideological Origins*  
*Terrorist and Para-State Organizations*  
*Terrorist Organization List, United States*  
*Terrorist Organizations, Freezing of Assets*

---

## Law Enforcement, Responses to Terrorism

---

The terrorist attacks of September 11, 2001, constituted a watershed event in American history, particularly for law enforcement. In the aftermath of that event, the nation's principal law enforcement officer, the attorney general, introduced new measures designed to prevent and combat terrorism, while the leading U.S. law enforcement agency, the Federal Bureau of Investigation (FBI), increasingly turned its intention toward terrorism. Through its Community Oriented Policing Services (COPS) program, which provides assistance and coordination to first responders at the local level, the Justice Department has helped state, county, and municipal forces respond to terrorism. The agencies have in turn developed a myriad of programs to improve intelligence collection and processing, increase the capacity to address terrorist acts, communicate with other public safety agencies, and respond to citizen fear while assisting victims.

### The Patriot Act

Following the attacks, Attorney General John Ashcroft drafted legislation known as the U.S. Patriot Act, which President George W. Bush signed into law on October 26, 2001. Controversial among civil libertarians, who regarded it as an erosion of freedoms, the 342-page bill contained changes to some 15 different statutes. Collectively, these changes gave the Justice Department and its agencies a number of new powers in intelligence gathering and criminal procedure against drug trafficking, immigration violations, organized criminal activity, money laundering, and terrorism and terrorism-related acts themselves.

Among its specific provisions, the Patriot Act gave increased authority to intercept communications related to an expanded list of terrorism-related crimes; allowed investigators to aggressively pursue terrorists on the Internet; provided new subpoena power to obtain financial



A 17-pound miniature helicopter created by a group of researchers at the Massachusetts Institute of Technology in 2002 could have future uses for civilian or military surveillance, shooting aerial camera footage, or scouting disaster areas and other dangerous terrain. AP/WIDE WORLD PHOTOS.

information; reduced bureaucracy by allowing investigators to use a single court order for tracing a communication nationwide; and encouraged sharing of information between local law enforcement and the intelligence community.

Prior to the Patriot Act, federal law had sharply limited the ability of prosecutors and law-enforcement officials to share investigative information with other federal officials, let alone local ones. Thanks to the Patriot Act, sharing would increase between intelligence organizations such as the Central Intelligence Agency (CIA), whose purview is international; the FBI, whose area of focus is domestic; and first responders, whose focus is the community. Such information sharing, it was hoped, would prevent information from falling through the cracks.

## The FBI

Allegations made by several special agents against their employer, the FBI, provided an example of the problems that occurred prior to the implementation of such information sharing. In July, 2001, Special Agent Kenneth Williams of the Phoenix FBI office sent his superiors a memo warning that Arab males with possible links to terrorist leader Osama bin Laden were training at an Arizona flight school. The bureau rejected his pleas for an investigation.

Around the same time, Special Agent Colleen Rowley of the Minneapolis office requested a warrant to conduct wiretaps and a computer search against an Arab trainee at a local flight school who had aroused suspicions when he told instructors that he only wanted to learn how to fly a plane, not how to land it. He was arrested for immigration violations in August, but still the bureau took little interest in Zacarias Moussaoui. Only after the September 11 attacks did authorities search the computer of the so-called “20th hijacker,” at which time they found phone numbers that might have led them to Moussaoui’s alleged co-conspirators.

**A new focus on counterterrorism.** The problem with the FBI was not incompetence or ignorance; rather, prior to September 2001, its mission had been strictly that of a law-enforcement agency. Its job was primarily to solve crimes that had already occurred, not to collect intelligence concerning terrorist attacks and other crimes that had yet to take place. Nor did it work closely with the CIA, because their missions were different, the one concerned with domestic affairs and the other focused on international concerns.

In the wake of September 11, Ashcroft and FBI Director Robert S. Mueller III refocused the bureau’s efforts

toward counterterrorism. In December, 2001, Mueller announced plans to reorganize headquarters by creating new counterterrorism, cybercrimes, and counterintelligence divisions; by modernizing information systems; and by emphasizing relationships with local first responders.

Criticized for not taking enough measures to direct the bureau toward its new mission, Mueller in the spring of 2002 announced a number of new reforms. These included the hiring of more analysts; the re-tasking of special agents to counterterrorism; the creation of an intelligence office; development of terrorism expert support teams to work with the bureau's 56 field officers; recruitment of Arabic speakers and others fluent in Middle Eastern and South Asian languages; creation of a joint terrorism task force to coordinate with the CIA and other federal agencies; and the improvement of financial analysis and other forms of strategic analysis directed toward terrorist groups.

## COPS, Local Law Enforcement, and Community Policing

Even as the nation's law enforcement leadership worked to refocus efforts toward combatting terrorism, the Justice Department had already put in place a program that greatly assisted local law enforcement in responding to terrorist acts and threats. This was COPS, which was already in place in September, 2001. COPS has helped local forces to strengthen their response to terrorism by improving data and intelligence collection and processing, capitalizing on technology advancements, encouraging communication with other public safety agencies, and helping local agencies to respond to citizen fear and prepare to assist potential victims.

As noted in a 2002 report on COPS programs, "Of course, these approaches are only one piece of the equation. A successful response to terrorism involves an array of activities, many of which are reliant on human intelligence gathering activities and productive partnerships between local law enforcement and other agencies." Still, COPS and similar federal programs have served to greatly improve the abilities of local forces to respond to situations. While each community force remains distinct, federal involvement increases the degree of coordination in activities.

Local forces have at their disposal a number of tools for managing data and intelligence, including in-field laptop computers, computer aided dispatch systems, enhanced records management systems, geographical information systems (GIS), and 311 phone systems. The last of these is aptly characterized by the tagline used to promote it in Chicago—the city's "other help line." In contrast to 911, the number set aside purely for emergencies, 311 is for

non-emergency calls to police, and for answering citizens' questions.

An example of an integrated information management system at the local level is the crime analysis workstation developed in Seattle through a 1997 COPS grant. Included in the station is crime-mapping software that can be used for traditional crime analysis (e.g., to detect patterns of burglary in a neighborhood), or adapted for emergency mobilization as in a terrorist situation. Under such conditions, peace officers might consult it to locate critical facilities such as fire stations and hospitals, or to provide emergency mobilization maps to all officers on patrol.

Crime mapping and information management can also be used to protect against terrorism, often by integrating law enforcement data (e.g., arrests, citations, and accidents) with non-law enforcement data such as financial and credit records, census information, tax and license registrations to businesses, and so on. Also included among varieties of non-law enforcement information is geographic data such as aerial photographs, floor plans, three-dimensional images of buildings, zoning and parcel information, and sewer and water systems.

By using such materials, authorities might, for instance, obtain information on companies such as plant nurseries or farm supply stores that serve as potential repositories for ammonium nitrate fertilizer, an ingredient used in many explosive devices. If a burglary were to occur at one of these facilities, this law enforcement information could be combined with the non-law enforcement information obtained earlier to track the possible use of ammonium nitrate for terrorist purposes. Similarly, if officials tracked a sharp increase in sales of flu medicine at drug stores, this might indicate that a biological attack had taken place.

## GIS and Crisis Management

Use of GIS applies geography, not so much to track criminal activity as to minimize and manage crises. Geographic information can be used to predict risks, and decrease loss of life and property, in the wake of a terrorist attack. It can also be used to develop target inventories and specific incident response scenarios, as well as to map out potential citizen evacuation routes. Use of GIS in integrated systems can enhance the coordination of law enforcement responses to crises.

In 1998, COPS provided a grant to Broward County, Florida, which used the funding to develop a means of information-sharing between local authorities and non-law enforcement first responders, such as firefighters and hospital emergency response teams, as well as law enforcement officials outside the local area. The Broward program included in-car mobile data computers and a

county-wide computerized dispatch system. Encompassed within this larger initiative was Operation Safe Schools, a software package provided to all first responders, which made possible the quick retrieval of floor plans, interior photographs, contact names and phone numbers, and evacuation routes for local schools.

In July, 2002, Representative Jim Saxton of New Jersey introduced the Law Enforcement Partnership to Combat Terrorism Act, designed to designate 25 percent of COPS funding toward intelligence programs. The move was another sign of the growing responsibilities placed on law enforcement in the post-September 11 world.

Since September, 2001, law enforcement has been encouraged, on the one hand, to be on the lookout for terrorists, but on the other hand, it is tasked with upholding the civil rights of persons unfairly targeted with suspicion. In the wake of the terrorist attacks, some civilians took it upon themselves to threaten, harass, or cause harm to persons of Middle Eastern descent or the Muslim faith. Along with these were other persons from south Asia who had no connection either to Islam or the Middle East. It is the role of police to prevent such hate crimes, and to enforce laws against them.

Similarly, law enforcement officers play a role in maintaining public calm, restoring order, providing a visible law enforcement presence, and answering requests for information and assistance. For the latter purpose, COPS in 2000 funded the National Center for Victims of Crime (NCVC), which operates a help line and distributes information cards. After September 11, the NCVC distributed half a million trauma information cards.

Not just the NCVC, but the entire system of incident response in the United States has been retasked since September 11, 2001. More than ever, first responders—law enforcement, firefighters, hospital emergency personnel, and others—will work together, as will agencies at the federal, state, and local levels. This integration of efforts will also see increased cooperation involving agencies whose role in upholding public security is not widely recognized by the general populace. Among these are the Environmental Protection Agency and the Nuclear Regulatory Commission, which, along with the Federal Emergency Management Agency and the Coast Guard, are involved in situations involving chemical, biological, and/or nuclear hazards.

#### ■ FURTHER READING :

##### BOOKS:

Campbell, Kurt M., and Michele A. Flournoy. *To Prevail: An American Strategy for the Campaign Against Terrorism*. Washington, D.C.: CSIS Press, 2001.

Chapman, Robert, et. al. *COPS Innovations: A Closer Look: Local Law Enforcement Responds to Terrorism: Lessons in Prevention and Preparedness*. Washington, D.C.:

U.S. Department of Justice Office of Community Oriented Policing Services, 2002.

##### PERIODICALS:

Eggen, Dan, and Jim McGee. "FBI Rushes to Remake Its Mission: Counterterrorism Focus Replaces Crime Solving." *Washington Post*. (November 12, 2001): A1.

##### ELECTRONIC:

Introduction of the Law Enforcement Partnership to Combat Terrorism. Federation of American Scientists. <[http://www.fas.org/irp/congress/2002\\_cr/h072902.html](http://www.fas.org/irp/congress/2002_cr/h072902.html)> (April 29, 2003).

Resources for Law Enforcement. Anti-Defamation League. <[http://www.adl.org/learn/additional\\_resources/default.asp](http://www.adl.org/learn/additional_resources/default.asp)> (April 29, 2003).

##### SEE ALSO

*Coordinator for Counterterrorism, United States Office FBI (United States Federal Bureau of Investigation)*  
*Food Supply, Counter-Terrorism*  
*Intelligence and Law Enforcement Agencies*  
*Justice Department, United States*  
*Law Enforcement Training Center (FLETC), United States Federal*  
*September 11 Terrorist Attacks on the United States*  
*United States, Counter-terrorism Policy*

---

## Law Enforcement Training Center (FLETC), United States Federal

---

The Federal Law Enforcement Training Center (FLETC) is an organization, rather than a single facility, dedicated to training personnel from some 75 federal law-enforcement agencies. In addition, it provides training to personnel from state, local, and international agencies, and to those from federal agencies not immediately tasked with law enforcement duties. In addition to its headquarters, at Glynco, Georgia, FLETC has a facility in Artesia, New Mexico, a temporary training center in Charleston, South Carolina, and a facility in development in Cheltenham, Maryland. Founded in 1970, FLETC is today part of the Department of Homeland Security.

Studies of federal law enforcement training during the 1960s showed the need for a uniform system of training. Not only would this standardize the training process across the many law-enforcement branches of the federal government, but also it would prove most cost-effective. This would in turn make it possible to develop a center





An instructor, background, teaches two Park Service Rangers the finer points of arresting a combative subject at the Federal Law Enforcement Training Center.

AP/WIDE WORLD PHOTOS.

where a talented and educated cadre of instructors could provide comprehensive training using modern facilities and a course content that would ensure the highest possible level of proficiency among students. The result was the establishment, in 1970, of the Consolidated Federal Law Enforcement Training Center (CFLETC) as a bureau of the Department of the Treasury.

Originally the headquarters of CFLETC, today known simply as FLETC, was to be in the Washington, D.C., area. After three years of construction delays, however, Congress requested a survey of surplus federal installations, and this resulted in planners reviewing the former Glynco Naval Air Station outside Brunswick, Georgia. In May 1975, Glynco was chosen as FLETC headquarters.

The Glynco campus, located between Savannah, Georgia, and Jacksonville, Florida, is similar to a town, and in fact it has its own zip code (31524). Included on the site are a practical exercise complex comprised of 34 buildings; enclosed firing ranges; a driver-training complex; numerous physical training areas; classroom buildings, which include laboratories and other specialized facilities; a computer resource learning center and library; and a television studio with the capability of broadcasting to field units throughout the United States and the world.

Glynco has a dining room where 4,000 meals are served each day. Included on the campuses are residence

halls, administrative buildings, and a wide array of recreational facilities for basketball, volleyball, tennis, soccer, billiards, ping pong, running, and swimming. There are also television lounges and a convenience complex that includes a barber shop, post office, laundry and dry cleaner, credit union, and convenience store. During the early 1990s, the center undertook a \$144 million expansion program.

FLETC added a second major facility in 1989, when the former Artesia Christian College campus in Artesia, New Mexico, became the FLETC Artesia Center. Artesia remains the principal advanced training facility for the Immigration and Naturalization Service (INS), U.S. Border Patrol, Bureau of Prisons, and other organizations with headquarters or large concentrations of personnel in the western United States. Artesia is similar to Glynco in the range of facilities offered, but it is smaller and houses fewer students at a time.

As a result of significant increases in the size of the INS and Border Patrol, mandated by Congress in 1995, FLETC needed a facility for training these officers. Planners chose the former Charleston Navy Base and Naval Weapons Station in Charleston. Renovation of the base began in January 1996 with the intention of developing a facility that would mirror Glynco. Training would continue at that facility for as long as the build-up of INS and Border Patrol officers continued.

Finally, in June 2001, FLETC chose a new site at the former Naval Communications Detachment facility in Cheltenham, Maryland. The 247-acre complex would become an area for firearms and vehicle operations requalification, and accordingly would contain facilities for simulations and exercises involving related skills. Construction began in late 2002, with completion scheduled for a year later.

The principal basic programs at FLETC are the Criminal Investigator Training Program; the Land Management Training Program, designed primarily for officers of agencies with a land management mission, such as the U.S. Forest Service or the National Park Service; and the Mixed Basic Police Training Program, which was created for uniformed services with a security or police mission, examples being the U.S. Secret Service Uniformed Division or the U.S. Capitol Police.

These and other programs at FLETC provide a combination of classroom instruction on hands-on practical exercises. Areas of study include firearms, driver training, physical techniques, legal, behavioral science, marine operations, enforcement operations and techniques, and security specialties. There are also advanced courses in specialized areas ranging from law enforcement photography to seized computers and evidence recovery.

In addition to training for federal, state, and local agencies—in some cases through specially designed agency-specific courses—FLETC offers training to foreign agencies. This training focuses on three main areas: the Law and Democracy Program of the U.S. government; the Antiterrorism Assistance Program; and the International Law Enforcement Academy sponsored by the Bureau for International Narcotics and Law Enforcement Affairs.

#### ■ FURTHER READING:

##### BOOKS:

Calhoun, Frederick S. *The Trainers: The Federal Law Enforcement Training Center and the Professionalization of Federal Law Enforcement*. Washington, D.C.: U.S. Government Printing Office, 1996.

##### PERIODICALS:

Johnson, Kevin. "Recruits Flood Federal 'Boot Camp'." *USA Today*. (September 23, 2002): A3.

"September 11 Leaves Facility Pushed to Its Maximum." *Augusta Chronicle* (Augusta, GA). September 2, 2002: B5.

##### ELECTRONIC:

Federal Law Enforcement Training Center. <<http://www.fleetc.gov>> (March 19, 2003).

##### SEE ALSO

*Homeland Security, United States Department United States, Intelligence and Security*

## Lawrence Berkeley National Laboratory (LBL)

■ K. LEE LERNER

The Lawrence Berkeley National Laboratory (LBL), located near the University of California Berkeley campus, is operated by the University of California for the United States Department of Energy (DOE).

Founded in 1931 by Nobel Prize-winning physicist Ernest Orlando Lawrence, LBL was designed to be a model for use of the interdisciplinary approach to scientific research. Initially dedicated to World War II military projects, in 1942, LBL became the first in a string of federal laboratories. Research at LBL brings scientists from a variety of disciplines to work on military and non-military funded projects. LBL scientists have developed a number of technologies related to national security interests, technology advancement, and environmental research.

LBL researchers developed a hand-held radiation detector that was able to distinguish between radioactive isotopes intended for biomedical research or clinical medical applications, and the form of isotopes most likely to be used by terrorists to construct a "dirty bomb" (a bomb that spreads radioactive materials by a non-nuclear explosion). The Cryo3 detector, developed in collaboration with researchers at Lawrence Livermore National Laboratory, employs radiation spectrometry to identify radioactive materials. The battery-powered unit utilizes a high purity germanium crystal that absorbs photons emanating from isotopes. By comparing differences in charge characteristics, the detector can further characterize both quantitative and qualitative attributes of a radioactive source. The development of new generations of detectors useful in identifying radioactive, chemical, and biological weapons detection remains a research interest. LBL researchers also developed a highly portable device capable of detecting explosives.

Although LBL's early work was heavily devoted to weapons research, in addition to making direct contributions to the technology of security, LBL scientists now engage in—and as an institution emphasize—a variety of research projects that advance both basic science and industry related projects to improve the quality of life.

The scientific divisions at LBL provide evidence of the emphasis on both physical and biological sciences. As of March 2003, LBL maintained divisions in Accelerator and Fusion Research; Advanced Light Sources; Chemical Sciences; Computational Research; Computing Sciences; Earth Sciences; Engineering; Environment, Health and Safety; Environmental Energy Technologies; Genomics; Information Technologies and Services; Life Sciences; Materials

Sciences; NERSC (National Energy Research Scientific Computing Center), Nuclear Sciences; Physical Biosciences; and Physics.

LBL scientists contributions to medical science and biotechnology include development of radiation therapies for treating cancer and research into HDL and LDL cholesterol physiology. LBL projects have also allowed a more complete understanding of how radon exposure increases cancer risk. Radon (usually in the form of the Radon-222 isotope) is a colorless and odorless radioactive gas formed from radioactive decay. The most common geologic source of radon derives from the decay of uranium. Radon is commonly found at low levels in widely dispersed crustal formations, soil, and water samples. Produced underground, radon moves toward the surface and eventually diffuses into the atmosphere or in groundwater. To some extent, radon can be detected throughout the United States. Specific geologic formations, however, frequently present elevated concentration of radon that may pose a significant health risk.

Scientists at LBL, Lawrence Livermore National Laboratory (LLNL), and Sandia National Laboratories California have also collaborated on the development of environmental remediation technologies useful in the cleanup of military disposal sites (e.g., the nearby Alameda Naval Air Station). LBL scientists also support the National Energy Research Scientific Computing Center (NERSC) (hosting the most powerful computer in the U.S. used for unclassified research) and an 88-inch cyclotron used to advance basic nuclear science.

#### ■ FURTHER READING:

##### ELECTRONIC:

Berkeley Lab. 88" Organization. 88-inch cyclotron. <<http://www.nsd.lbl.gov/LBL-Programs/nsd/user88/>> (March 23, 2003).

Berkeley Lab Research News. "DOE's NERSC Center deploys 10 teraflops per second IBM supercomputer." March 10, 2003. <<http://www.lbl.gov/Science-Articles/Archive/NERSC-10-teraflop-IBM.html>> (March 23, 2003).

United States Department of Energy, Office of Science. National Laboratories and User Facilities. <[http://www.sc.doe.gov/Sub/Organization/Map/national\\_labs\\_and\\_userfacilities.htm](http://www.sc.doe.gov/Sub/Organization/Map/national_labs_and_userfacilities.htm)> (March 23, 2003).

United States Department of Homeland Security. Research & Technology. <<http://www.dhs.gov/dhspublic/display?theme=27&content=374>> (March 23, 2003).

University of California. Department of Energy National Laboratories. <<http://www.universityofcalifornia.edu/labs/>>(March 22, 2003).

#### SEE ALSO

*Argonne National Laboratory*  
*Brookhaven National Laboratory*

*DOE (United States Department of Energy)*  
*Environmental Measurements Laboratory*  
*Lawrence Livermore National Laboratory (LLNL)*  
*Los Alamos National Laboratory*  
*NNSA (United States National Nuclear Security Administration)*  
*Oak Ridge National Laboratory (ORNL)*  
*Pacific Northwest National Laboratory*  
*Plum Island Animal Disease Center*  
*Sandia National Laboratories*

## Lawrence Livermore National Laboratory (LLNL)

■ K. LEE LERNER

The Lawrence Livermore National Laboratory (LLNL), located near the University of California Berkeley campus, is operated by the University of California for the United States Department of Energy (DOE).

Founded in 1952, LLNL initially served as a nuclear weapons research and development facility. Research eventually expanded to serve a wider scope of science and engineering projects. Although LLNL's primary mission is to develop technologies that safeguard U.S. nuclear weapons, LLNL applications are also used to prevent proliferation of nuclear weapons technology and to verify existing treaties regarding nuclear weapons development and testing. In addition, LLNL research projects serve biomedical research and environmental interests.

LLNL responsibilities for nuclear weapons safety also include ensuring that the stockpile of U.S. weapons remains reliable. This role became especially important after the U.S. committed to a comprehensive nuclear test ban in 1995. As part of its Stockpile Stewardship and Management Program (SSMP), LLNL must certify the reliability of nuclear weapons without detonation testing. SSMP programs also involve scientists and engineers from Los Alamos National Laboratory (LANL), Sandia National Laboratories, and production facilities at Pantex, Savannah River, Kansas City, and Oak Ridge.

LLNL personnel maintain a special interest in predicting the impact of aging on the nuclear stockpile. Weapons-grade uranium, plutonium, and subcritical elements change over time and preventing weapon degradation is a critical concern in ensuring weapon reliability. LLNL developed ultrashort-pulse laser technology, which provides for more efficient use of weapons-grade materials used to refurbish weapons. Certification of the nuclear stockpile requires separate and independent inspections by at least two SSMP component laboratories. The dual certification approach enhances inspection confidence.

LLNL scientists and engineers are also responsible for weapons design, subcritical testing (nonexplosive testing) at the Nevada Test Site (a nuclear weapons test site adjacent to the Nellis Air Force range complex located approximately 65 miles from Las Vegas), and the development of sensors that can be utilized in noninvasive and nondestructive weapons surveillance tests. Highly sensitive standoff sensors allow the accurate measurement from a safe distance of trace amounts of airborne contaminants emanating from a suspected weapons facility. In addition, low-level radiation sensors help identify potential nuclear threats. LLNL hydrodynamic experiments allow scientists to evaluate explosive detonation and implosion phases in the nuclear detonation sequence.

Other LLNL facilities include a High Explosives Applications Facility, Nova Laser Facility, Flash X-Ray Facility, and the National Ignition Facility (NIF) that hosts the largest laser in the world. High-speed supercomputer facilities that are a part of the Accelerated Strategic Computing Initiative (ASCI) allow improved modeling and database assembly.

To facilitate the identification of biological weapons, LLNL scientists developed a mini-PCR (polymerase chain reaction) test that can be used for *in situ* analysis. Polymerase chain reaction is a technique in which cycles of denaturation, annealing with primer, and extension with DNA polymerase, are used to amplify the number of copies of a target DNA sequence by hundreds of times in just a few hours.

Environmental safety is enhanced by LLNL initiatives in plutonium disposal.

In addition to developing technologies utilized in monitoring the Comprehensive Test Ban Treaty, LLNL programs also develop technologies used to monitor the Chemical Weapons Convention. LLNL scientists are actively involved in securing the former Soviet Union nuclear stockpile now held by the Russian Federation.

## ■ FURTHER READING:

### ELECTRONIC:

Lawrence Livermore National Laboratory. March 24, 2003. <<http://www.llnl.gov/>> (March 24, 2003).

United States Department of Energy, Office of Science. National Laboratories and User Facilities. <[http://www.sc.doe.gov/Sub/Organization/Map/national\\_labs\\_and\\_userfacilities.htm](http://www.sc.doe.gov/Sub/Organization/Map/national_labs_and_userfacilities.htm)> (March 23, 2003).

United States Department of Homeland Security. Research & Technology. <<http://www.dhs.gov/dhspublic/display?theme=27&content=374>> (March 23, 2003).

### SEE ALSO

*Argonne National Laboratory*  
*Brookhaven National Laboratory*

*DOE (United States Department of Energy)*  
*Environmental Measurements Laboratory*  
*Lawrence Berkeley National Laboratory*  
*Los Alamos National Laboratory*  
*NNSA (United States National Nuclear Security Administration)*  
*Oak Ridge National Laboratory (ORNL)*  
*Pacific Northwest National Laboratory*  
*Plum Island Animal Disease Center*  
*Sandia National Laboratories*

## League of Nations

■ ADRIENNE WILMOTH LERNER

When the United States entered World War I in 1917, President Woodrow Wilson declared that the nation's intention was to fight in the final war to ensure the survival and strength of democracy in the Western world. After the war, Wilson encouraged the victorious Allied powers to establish an international organization that would mediate conflict through diplomacy and promote peace. Wilson's idea led to the creation of the League of Nations, and earned him the Nobel Peace Prize in 1919. The League of Nations was short lived, and plagued with problems from its inception. The organization did, however, lay the foundations for international cooperative efforts in the latter half of the twentieth century.

Despite Wilson's efforts to gain public support for the League of Nations, the United States government failed to ratify the Treaty of Versailles, the final agreement of the ending of World War I, and therefore, did not join the League. The lack of United States participation and financial backing forever plagued the League, hampering its efficacy and political influence. United States abstention from the League drew ire from some nations, and made others suspicious of the organization itself. Britain expressed dissatisfaction with the League, but ratified the treaty with the League of Nations provisions simply to avoid extended negotiation on reforming the already delayed peace settlement. Despite U.S. reservations, over 30 other nations joined the League in 1920 when the Treaty of Versailles went into effect on January 10: Australia, Belgium, Bolivia, Brazil, Britain, Canada, China, Cuba, Czechoslovakia, Ecuador, France, Greece, Guatemala, Haiti, Hejaz, Honduras, Italy, India, Japan, Liberia, New Zealand, Nicaragua, Panama, Peru, Poland, Portugal, Romania, Serb-Croat-Sloven State (later, Yugoslavia), Siam, South Africa, and Uruguay.

The League was headquartered in Geneva, Switzerland, because of the nations long-standing policy of declared neutrality. Though the Treaty of Versailles provided

for the establishment of the diplomatic entity, it did not outline its organization. Its eventual structure took shape over the first two years of representative meetings of member nations. Eventually, the League came to be composed of three principal organs and several technical organizations.

The main body of the League of Nations was the assembly. Composed of representatives from each member state, the assembly met annually. Each resolution, or legal advisory, passed by the assembly was subsequently published.

The council was a smaller body of representatives separate from, but still accountable to, the assembly. Membership on the council varied, and included a mixture of permanent and non-permanent seats. The mission of the council was to mediate and settle international disputes. The League of Nations charter stipulated that the council meet every four years, or as needed in the event of a crisis. In the League of Nations's 20-year history, the council met 107 times.

The secretary-general directed the League of Nations, serving as its chief negotiator and the leader of the assembly. The office of the secretary-general, the secretariat, carried out the routine office work of the league.

In addition to the principal organs of the league, several technical committees advised the assembly and council on international policy and special concerns. The league maintained a health organization, an economic and financial organization, the Opium Advisory Committee, and the Permanent Mandates Commission, in addition to several other temporary groups.

In its two-decade tenure, the League of Nations produced the first truly international laws and cooperative initiatives. The League Health Organization promoted safe hospital practices, vaccination campaigns, and public health information campaigns to curb the spread of venereal disease and tuberculosis. In response to the horrors of poison gas on the World War I battlefield, member nations negotiated bans on chemical weaponry. The rules of engagement for war were modified and codified for the modern era in the terms of the Geneva Convention. The league prompted member states to adhere to its terms, but to avoid war if possible.

In the mid-1930s, the league became increasingly ineffective. Though several nations attempted to halt the spread of Nazism, Fascism, and Communism through diplomacy, their efforts failed to prevent the outbreak of World War II in 1939. The league met for the last time during the war, and was dissolved by its member states on April 18, 1946.

Despite its limitations, the League of Nations established modern, international diplomatic protocol and fostered increasing cooperation between large and small nations on both sides of the Atlantic. Participation in the

league drew some nations out of isolationism and propelled others onto the international economic and political stage. After the dissolution of the League of Nations, another international and legal entity, the United Nations, emerged. The atrocities of the Holocaust and a rise in war crimes prompted the international community to establish a body that could define and administer international law. The United States joined the United Nations as a charter member, officially ending its remnant isolationist policies. The United Nations assumed the duties of the former League of Nations and continues to expand its role in international diplomacy.

#### ■ FURTHER READING:

##### BOOKS:

Knock, Thomas A. *To End All Wars*, reprint ed. Princeton, N.J.: Princeton University Press, 1995.

##### SEE ALSO

*United Nations Security Council  
World War I*

---

## Lebanon, Bombing of U.S. Embassy and Marine Barracks

---

On two occasions in 1983, terrorists bombed United States targets in Beirut, Lebanon. The first target, on April 18, was the U.S. embassy, where 63 people, including 17 Americans, were killed. Half a year later, on October 23, the terrorists struck again, this time at barracks that housed members of an international peacekeeping force sent to help restore order in the war-torn nation. Killed in this second attack were 242 U.S. Marines, along with 58 French troops. Until September 11, 2001, the October 1983 assault would remain the most devastating terrorist attack on American citizens, and it remains the bloodiest terrorist assault on Americans outside of the United States. The group Islamic Jihad, affiliated with Hezbollah and ultimately Iran, claimed responsibility for both attacks.

The April attack, along with the simultaneous assaults on U.S. and French barracks in October, were all suicide bombings using vehicles laden with explosives. In the first bombing, the vehicle was a van that had reportedly been stolen from the embassy in June of the preceding year. At lunchtime on April 18, it slammed into the side of the seven-story building, and the driver detonated 2,000 pounds of explosives. The blast tore away the front portion of the building, leaving a site that looked much as the



U.S. Marines and an Italian soldier, right, dig through the debris at battalion headquarters in Beirut after the bombing. AP/WIDE WORLD PHOTOS.

Alfred P. Murrah Federal Building in Oklahoma City would after the attack there 12 years later. Among the dead were the entire U.S. Central Intelligence Agency Middle East contingent, several State department officials (including three USAID employees), several U.S. Army trainers and a Marine embassy guard, and journalist Janet Lee Stevens.

In the October 23 attacks, the terrorists struck two targets simultaneously, a maneuver that would be replicated by al Qaeda in the bombing of U.S. embassies in Africa 15 years later. The attack occurred on a Sunday morning at 6:22 a.m. local time, when a large Mercedes truck burst through the barrier surrounding the Marine compound and slammed into the first floor of the four-story concrete building. The driver then detonated his 12,000-pound bomb. At almost the same moment, a 400-pound bomb carried by a pickup truck exploded outside the nine-story French barracks.

The attack occurred just as the United States launched its first significant military operation since the end of the Vietnam War 10 years earlier: the assault on Grenada, a Caribbean island that had fallen under the control of a Marxist regime. Perhaps because of divided attention, combined with the sensitive nature of relationships in Lebanon, at that time a veritable no-man's land of warring factions, the United States took no significant overt retaliatory action against Islamic Jihad.

#### ■ FURTHER READING:

##### BOOKS:

- Frank, Benis M. *U.S. Marines in Lebanon, 1982–1984*. Washington, D.C.: U.S. Marine Corps, 1987.
- Hammel, Eric M. *The Root: The Marines in Beirut, August 1982–February 1984*. San Diego: Harcourt Brace Jovanovich, 1985.
- Jenkins, Brian Michael. *The Lessons of Beirut: Testimony Before the Long Commission*. Santa Monica, CA: Rand Corporation, 1984.
- Petit, Michael. *Peacekeepers at War: A Marine's Account of the Beirut Catastrophe*. Boston: Faber and Faber, 1986.

##### ELECTRONIC:

- Beirut Memorial Online. <<http://www.beirut-memorial.org/history/>> (April 7, 2003).

##### SEE ALSO

- Cold War (1972–1989): The Collapse of the Soviet Union*
- Iran, Intelligence and Security*
- Israel, Intelligence and Security*
- Kenya, Bombing of United States Embassy*
- Libya, U.S. Attack (1986)*
- Middle East, Modern U.S. Security Policy and Interventions*

*Reagan Administration (1981–1989), United States National Security Policy  
Syria, Intelligence and Security*

## Less-Lethal Weapons Technology

■ JUDSON KNIGHT

Less-lethal weapons are tools and techniques designed for riot control and other security functions with the intention of neutralizing hostile activity without killing or causing permanent bodily harm. Varieties of less-lethal weapons technology range from batons and beanbag rounds (non-lethal bullets fired from an ordinary or modified rifle or shotgun) to electric Tasers, pepper spray and tear gas, and equipment that emits loud noises, bright lights, or even bad smells. Supporters of less-lethal weapons technology maintain that it constitutes a humane means of controlling disturbances, but detractors hold that these weapons are more harmful than authorities claim.

### A Survey of Less Lethal Weapons

The array of technologies under the heading of “less-lethal weapons” is vast. As early as 1972, a report by the U.S. National Science Foundation identified no less than 34 varieties of less-lethal weapons technology then in the research or developmental stages. Among these were electrified water jets; stroboscopic light and pulsed sound weapons; infrasound weapons which would use low-frequency noises inaudible to the human ear; guns for firing drug-filled rounds; “stench darts,” which would emit a powerful and unpleasant smell; and a device called an “instant banana peel,” designed to make pavement slippery. A later weapon in development at the beginning of the twenty-first century used sticky foam which, when fired at an attacker, made it impossible for the attacker to move.

Among the most well known of devices is the M26 Advanced Taser, which can be used to neutralize an individual by means of electric shock. Similarly, electronic riot shields and electroshock batons also use voltage to neutralize attackers. Manufactured since the mid-1980s, electrified riot shields make use of special plates fitted with metal strips. In the handle of the shield is a button which, when pushed, can send as much as 100,000 volts—twice the capacity of an ordinary Taser—through the metal, an act accompanied by the emission of loud noises and bright sparks.

Numerous varieties of less-lethal devices are fired from an ordinary rifle or shotgun, or one that has been modified for that purpose. This technology originated with British colonial forces in Hong Kong, who used wooden

rounds. Varieties of less-lethal ammunition include baton rounds or plastic bullets; wooden bullets; rubber balls; and nylon bags filled with lead pellets known as “beanbag” rounds.

**Sounds, smells, and light.** Numerous varieties of less lethal weapons technology make use of sounds, smells, or light. The basic idea behind such techniques is not new; biblical texts report that prior to attacking the city of Jericho, the Israelites marched around it seven times, shouting and smashing cymbals to intimidate the inhabitants. In World War II, the U.S. Office of Strategic Services (OSS) issued to its operatives in Asia a “psychological harassing agent” called “Who, Me?” According to an OSS manual, the gas “is to be squirted directly upon the body or clothing of a person a few feet away. The odor is that of Occidental feces, which is extremely offensive...”

In the late twentieth century, a British government research project was tasked with developing means of using noxious odors for crowd control in Northern Ireland. Among the items in development, according to a *Financial Times* report, were chemical compounds intended to produce “transient symptoms of nausea and gagging.” The principal is not different from that of tear gas and pepper spray (itself a variety of tear or CS gas), chemicals long used to quell riots or neutralize attackers.

Researchers at U.S. national laboratories are also reportedly in the process of developing various means for using sound and light as weapons. For example, ultrasound generators, as well as microwave and acoustic disabling systems, may be used to disturb the inner ear, throwing an individual off balance. Another item of future technology is a radiator shell that would use superheated gaseous plasma, or ionized gas, to produce bursts of light.

### Controversy

In discussing less-lethal weapons technology, there is little middle ground. On the one hand, law enforcement agencies and supporters present these materials and techniques as humane alternatives to more violent means of crowd control. On the other hand, opponents view them as methods by which a police state can potentially exert greater power over its subjects.

The antipathy toward less-lethal weapons technology by environmental, socialist, and anarchist groups is not surprising, given the fact that protesters associated with these movements have most often been the target of less-lethal weapons. They have been used, for instance, to quell anti-globalization demonstrations in recent years, as well as antiwar protests in the United States during the 2003 war in Iraq.

Unfortunately, discussion of less-lethal weapons technology, pro or con, is limited beyond the ranks of extremist groups. Reports in law enforcement journals tend to be confined largely to scientific evaluation of the weapons’



An executive with American Technology Corporation displays a type of sound-gun device that can beam sound to a person so that it appears to be coming from a wall or other inanimate object. Soldiers may someday have similar non-lethal weapons in their arsenals. AP/WIDE WORLD PHOTOS.

effectiveness, rather than to questions of whether they meet designers' putative aim of providing more humane control systems.

A 2002 *Law & Order* review of less-lethal weapons did, however, note that "while they do greatly reduce the risk that a subject will be killed, the risk is still unfortunately present." For this reason, the National Tactical Officers Association had undertaken a study to assess the causes of deaths from less lethal weapons, and to develop means of reducing the dangers. "In the interim," the report noted, "one of the best things that departments can do is [to] restrict the use of these projectiles to the upper end of the force spectrum."

#### ■ FURTHER READING:

##### PERIODICALS:

Eaglesham, Jean. "Bad Smells' Could Be Used to Disperse Crowds." *Financial Times*. (October 31, 2002): 3.  
"IACP's Less Lethal Force Options Course." *Law & Order* 49, no. 9 (September 2001): 95-99.

Oldham, Scott. "Less-Lethal Munitions." *Law & Order* 50, no. 2 (September 2002): 54-56.

Rappert, Brian. "Assessing Technologies of Political Control." *Journal of Peace Research* 36, no. 6 (November 1999): 741-750.

Rosenbarger, Matt. "Less-Lethal Improvements: Federal and ALS Work Together." *Law & Order* 49, no. 11 (November 2001): 84-86.

##### ELECTRONIC:

An Appraisal of Technologies of Political Control. <<http://cryptome.org/stoa-atpc.htm>> (April 15, 2003).

## L-Gel Decontamination Reagent

#### ■ BRIAN HOYLE

L-Gel is a coating that was developed at Lawrence Livermore National Laboratory (LLNL) in Berkeley, California.





An old baton round, left, and one of the new baton rounds, right, also known as plastic bullets. The plastic bullets expand upon contact and release most of their destructive energy before penetrating vital organs.  
AP/WIDE WORLD PHOTOS.

The coating is effective at decontaminating areas exposed to both chemical and biological agents.

The need to decontaminate spills of a liquid or powdered poison or infectious organism is potentially urgent. In order to prevent injury from chemical or biological warfare agents, for example, the source agent must be contained before anyone touches the material, or before the agents become dispersed in air currents. For example, a spill of powdered anthrax spores can become airborne if not contained quickly, and could travel throughout a building's ventilation system.

The development of L-Gel began in the 1990s. Among those striving to develop a nonhazardous, portable, and inexpensive decontamination reagent were LLNL researchers. Their L-Gel formulation incorporates a chemical compound called potassium peroxymonosulfate into a material called silica.

Potassium peroxymonosulfate is an oxidant. That is, it contributes an electron to the chemical bonds of the target compound, which disrupts the bonds that hold the target together or make it active. Bleach is another oxidant. However, bleach produces noxious fumes, making its use in confined settings dangerous. Bleach is also corrosive, and could damage equipment that is being decontaminated.

The acidic nature of the peroxymonosulfate oxidant proved effective against a variety of biological agents, including anthrax spores. Spores such as those of anthrax have several hard coats that are very resistant to chemicals and physical stresses such as heat, ultraviolet light, and temperature. Acidic oxidants, however, can break apart the proteins that make up the outer coats. The oxidizer can then enter the core of the spore, which houses the genetic material, and can destroy the nucleic acid that is vital for the germination of the spore into a growing and infectious bacterium.

The oxidant is incorporated into a gel. The thick gel is able to cling to surfaces better than water, and remains where it has been applied. A water-based solution will spread out and could even run down an inclined surface, which could further disperse the poison or infectious microbe. Another advantage of a gel is that the oxidant is kept in contact with the target longer than would be possible if the oxidant was dissolved in water.

L-Gel is effective at killing over 99% of populations of bacteria including *Bacillus anthracis* (the bacterium that causes anthrax) and *Yersinia pestis* (the bacterium that causes plague). Surfaces as varied as carpet, wood, and stainless steel are all efficiently decontaminated with L-Gel.

During the fall of 2001, letters containing anthrax spores were sent to a number of locations in the eastern United States. L-Gel was successfully used to decontaminate offices of Congress and at the American Broadcasting Company's (ABC) newsrooms.

Research is underway to produce L-Gel capsules that could be blown into ventilation ducts, where clean up of chemical and biological agents is especially difficult.

#### ■ FURTHER READING:

##### PERIODICALS:

Raber, E. "L-Gel Decontaminates Better Than Bleach." *Science and Technology Review*. (March 2002): 10–16.

##### SEE ALSO

*Biocontainment Laboratories*  
*Decontamination Methods*  
*Pathogens*

---

## Liberation Tigers of Tamil Eelam (LTTE)

---

The Liberation Tigers of Tamil Eelam (LTTE), also known as the World Tamil Association (WTA), World Tamil Movement (WTM), the Federation of Associations of Canadian Tamils (FACT), the Ellalan Force, and the Sangilian Force, was founded in 1976. LTTE is the most powerful Tamil

group in Sri Lanka and uses overt and illegal methods to raise funds, acquire weapons, and publicize its cause of establishing an independent Tamil state. The LTTE began its armed conflict with the Sri Lankan government in 1983 and relies on a guerrilla strategy that includes the use of terrorist tactics.

### Other names

The Tigers have integrated a battlefield insurgent strategy with a terrorist program that targets not only key personnel in the countryside, but also senior Sri Lankan political and military leaders in Colombo and other urban centers. The Tigers are most notorious for their cadre of suicide bombers, the Black Tigers. Political assassinations and bombings are commonplace. The LTTE has refrained from targeting foreign diplomatic and commercial establishments but maintains an active media effort.

The exact strength of LTTE is unknown, but it is estimated to have 8,000 to 10,000 armed combatants in Sri Lanka, with a core of trained fighters of approximately 3,000 to 6,000. The LTTE also has a significant overseas support structure for fundraising, weapons procurement, and propaganda activities.

The Tigers control most of the northern and eastern coastal areas of Sri Lanka but have conducted operations throughout the island. Headquartered in northern Sri Lanka, LTTE leader Velupillai Prabhakaran has established an extensive network of checkpoints and informants to keep track of any outsiders who enter the group's area of control.

The LTTE's overt organizations support Tamil separatism by lobbying foreign governments and the United Nations. The LTTE also uses its international contacts to procure weapons, communications, and any other equipment and supplies it needs. The LTTE exploits large Tamil communities in North America, Europe, and Asia to obtain funds and supplies for its fighters in Sri Lanka, often through false claims or even extortion.

### ■ FURTHER READING:

#### ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001. Annual Report: On the Record Briefing. May 21, 2002 <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

#### SEE ALSO

*Terrorism, Philosophical and Ideological Origins*  
*Terrorist and Para-State Organizations*  
*Terrorist Organization List, United States*  
*Terrorist Organizations, Freezing of Assets*

## Libraries and Information Science (NCLIS), United States National Commission on

The membership of the commission consists of the Librarian of Congress and fourteen other members who serve five-year terms. Five members of the commission are required to be professional librarians or information science specialists. Other members can be non-professionals, but must have distinguished themselves as having a special dedication to literacy causes, library technology, or information services. Several well-known authors and celebrity champions of literacy have served on the commission. Three committee members are designated to oversee policy addressing information access and literacy issues of the handicapped, elderly, and children. All members are appointed to the position by the President, and approved by the legislature.

During the 1990s, the commission focused on formulating policies and guidelines for the use of technology in library systems. The advent of the internet created new opportunities for the creation of electronic information storage and dissemination. As individual libraries, including the Library of Congress, converted their own directory systems from paper to electronic indices, NCLIS issued advisory guidelines addressing equal access concerns for the vision and hearing impaired. Internet access and electronic databases of government information within library systems was the focus of a 1995 committee study, with special attention paid to numerous security issues. The committee endeavors to make public-domain government information readily available through the library system, but also advises on security measures to adequately curate more sensitive information.

In 2001, the NCLIS undertook a study of the distribution and dissemination of government archives and information in national, state, local, and school library systems. After the September 11 terrorist attacks, the NCLIS drafted a policy on the availability and dissemination of terrorism readiness and prevention information.

### ■ FURTHER READING:

#### ELECTRONIC:

United States National Commission on Libraries and Information Science. <<http://www.nclis.gov/about/about.cfm>>(1 December 2002).

## Libya, Intelligence and Security

Libya, under the leadership of Colonel Muammar Abu Minyar al-Qadhafi, espouses a political theory that combines elements of socialism and fundamentalist Islamic law. Qadhafi promoted his political system, which he dubbed the Third International, by a series of military incursions into neighboring Chad and sponsoring anti-capitalist terrorist organizations. Throughout the 1980s, Libya garnered international scorn for its policy of state-sponsored terrorism. In 1992, the United Nations imposed strict sanctions on the nation, including a ban on all its international air traffic.

Under Qadhafi's rule, Libya's intelligence community was reorganized into a militarized force. Intelligence and police forces engage in political espionage, ferreting out dissident groups. Libyan intelligence was also accused by members of the international community for training terrorist operatives and paramilitary agents.

The main agency of Libyan intelligence is the Military Intelligence Force. Military intelligence collects both foreign and domestic intelligence information. Most intelligence forces operate as strategic, special units, whose daily operations remain largely unknown.

The Secretariat of the Interior administers intelligence services responsible for the preservation of national security, and protection of government buildings and officials. A variety of specialized police forces, including the People's Security Force and the National Police, combine intelligence and law enforcement duties. However, elite elements of these Special Branch Units also operate as secret police forces, arresting and detaining any individuals suspected of anti-government activity.

Tensions between Libya and Western nations escalated throughout the 1980s and 1990s. In April, 1986, The U.S. launched a series of air strikes upon military targets in Libya, destroying command centers and military bases that were directly linked through intelligence sources to terrorist training and operations. The strikes, codenamed El Dorado Canyon, were carried out ten days after a bomb exploded in a discotheque frequented by American military personnel, where one American died and 63 others were among the over 200 injured. American intelligence officials had previously intercepted a message from Qadhafi ordering the attack.

Libya withdrew its military forces from Chad in the late 1980s, but then attempted to sabotage Western-Arab relations by interfering with ongoing peace negotiations between Israel and the Palestinian Authority. The Libyan government called upon Arab nations to stall the Middle East peace process through acts of terrorism and the repatriation of Palestinian refugees. In return, the United States government enacted strict laws prohibiting U.S.

companies from doing business in Libya or with Libyan companies.

Under the yoke of sanctions, Libya extradited two suspected terrorists for trial in the Netherlands. The act prompted the UN to ease, and then suspend sanctions. In July of 2000, Libya resumed air travel to Morocco and Egypt. Following the September 11, 2001, terrorist attacks on the United States, however, Libya's state-sponsorship of Islamist terrorist organizations, and their resumed relations with Iraq, drew sharp criticism from the United States and British governments.

### ■ FURTHER READING:

#### ELECTRONIC:

CIA World Factbook. "Libya." <<http://www.cia.gov/cia/publications/factbook/geos/ly.html>> (April 28,2003).

## Libya, U.S. Attack (1986)

The United States air assault on Libya in April 1986 marked the first major American military response to modern terrorism. The immediate cause was a terrorist bombing in West Berlin ten days earlier, an incident to which U.S. intelligence sources linked Libyan strongman Muammar Qadhafi. The response of President Ronald Reagan was a massive bombing raid on facilities in Tripoli and Benghazi, the country's two major cities. Although the 1986 attacks did not bring an end to Qaddafi's state-sponsored terrorism—the 1988 bombing of Pan Am flight 103 over Lockerbie, Scotland, occurred less than two years later—it marked the first step on a long road toward open confrontation with terrorism and terror-sponsoring states.

**Early provocations.** Qadhafi seized power in 1969, and during the 1970s and 1980s used his oil wealth to sponsor terrorist movements in 50 or more countries from Northern Ireland to the Philippines. He also undertook other aggressive moves, such as his declaration in 1973 that the Gulf of Sidra between Tripoli and Benghazi belonged to Libya.

The United States refused to recognize this claim, and in August 1981—on orders from Reagan—the U.S. Sixth Fleet conducted exercises in the gulf. The result was a skirmish between two U.S. F-14 Tomcat fighters and two Soviet-made Su-22 fighter-bombers. The Americans shot down both Libyan planes, whose pilots ejected and were rescued by their own forces; the incident proved the superiority of Sidewinder missiles over Soviet Atoll air-to-air missiles.

**Operation El Dorado Canyon.** Over the course of the next five years, tensions grew between the Reagan administration and the Qadhafi regime, which increased its sponsorship of and direct involvement in terrorism. On March 24, 1986, Libya launched six SA-5 missiles against the U.S. Sixth Fleet, which was conducting maneuvers nearby in the Mediterranean. The attacks failed, and in subsequent strikes and counterstrikes, the Americans sunk two Libyan vessels. On April 5, 1986, a bomb exploded in Berlin's La Belle discotheque, killing a U.S. soldier and a Turkish civilian, and injuring some 200 others, including 63 U.S. soldiers.

Ten days later, late in the evening of April 15, the United States prepared for air strikes against Libyan ground targets in five areas: the Aziziya barracks, known as a command and control post for terrorist activities; the military facilities at the Tripoli international airport; the Side Bilal base, said to be a facility for training terrorists in underwater sabotage; the Jamahariya military barracks in Benghazi, another terrorist command post; and the Benina air base southeast of Benghazi.

The attack, known as Operation El Dorado Canyon, involved more than 100 U.S. aircraft. The principal strike force was in the form of Navy A-6s from the aircraft carriers USS *America* and USS *Coral Sea*, and Air Force F-111s from airbases in the United Kingdom. The refusal of the French government to grant authority for an American overflight of their country greatly complicated matters, and necessitated refueling of the aircraft in a much longer flight around the Iberian peninsula.

Despite this obstacle, the U.S. force was able to launch its attack at 2:00 a.m. local time on April 16. Over the course of 12 minutes, U.S. forces dropped 60 tons (61 tonnes) of munitions and encountered negligible resistance from the Libyans, who failed to get a single aircraft airborne to challenge the attackers.

**Aftermath.** Qadhafi's agents later took part in the Lockerbie bombing, but for the most part his interest in international terrorism cooled after April 1986. After a protracted battle of words, in March 1999 he agreed to turn over two suspects in the Lockerbie bombing but claimed that the Americans who carried out the 1986 bombing raids should be charged for killing 31 people and wounding 226 others.

In May 2001, Qadhafi admitted to a German newspaper that Libya had been behind the discotheque bombing 15 years earlier, an apparent act of retaliation for the U.S. sinking of the two vessels in March 1986. In the La Belle bombing, he had received help from the East German Stasi intelligence service, but according to Stasi files retrieved after the end of the Cold War, the East Germans actively discouraged Middle-Eastern terrorism in Germany following the April 1986 U.S. retaliation against Libya. The La Belle bombing case, which could not have been possible prior to German reunification, finally went to trial in 2001, and in November, a German court found four people guilty of the attacks. They included a German woman and

three men: a Palestinian, a Lebanese-born German, and a Libyan.

#### ■ FURTHER READING:

##### BOOKS:

Davis, Brian L. *Qaddafi, Terrorism, and the Origins of the U.S. Attack on Libya*. New York: Praeger, 1990.

Venkus, Robert E. *Raid on Qaddafi: The Untold Story of History's Longest Fighter Mission by the Pilot Who Directed It*. New York: St. Martin's Press, 1992.

##### PERIODICALS:

Greenberger, Robert S. "Dictating Terms: Sept. 11 Aids Gadhafi in Effort to Get Libya off U.S. Terrorist List." *Wall Street Journal*. (January 14, 2002): A1.

Herschensohn, Bruce. "What Proof? Terrorism Alone Is Cause for Action." *Los Angeles Times*. (October 5, 2001): B15.

Weinberger, Caspar, and Peter Schweizer. "...But We've Defeated Terrorists Before." *USA Today*. (September 24, 2001): A15.

Williamson, Hugh. "Libya Blamed for 1986 Berlin Disco Bombing." *Financial Times*. (November 14, 2001): 12.

##### ELECTRONIC:

Operation El Dorado Canyon. Federation of American Scientists. <[http://www.fas.org/man/dod-101/ops/el\\_dorado\\_canyon.htm](http://www.fas.org/man/dod-101/ops/el_dorado_canyon.htm)> (April 7, 2003).

##### SEE ALSO

*Aircraft Carrier*  
*Cold War (1972–1989): The Collapse of the Soviet Union*  
*Enduring Freedom, Operation*  
*Iraqi Freedom, Operation (2003 War Against Iraq)*  
*Libya, Intelligence and Security*  
*Pan Am 103 (Trial of Libyan Intelligence Agents)*  
*Reagan Administration (1981–1989), United States National Security Policy*

## LIDAR (Light Detection and Ranging)

LIDAR is an active remote sensing system that allows exceptionally accurate and rapid determination of terrain and structural features (e.g. height). LIDAR produces highly accurate three-dimensional data measurements that can then be utilized by mapping, guidance, and navigation systems. For example, LIDAR data utilized by Geographic Information Systems (GIS) software, and coordinated with differential Global Positioning System (GPS) data can produce extremely accurate terrain maps that be integrated with other tactical data (e.g. location of targets, etc).

LIDAR technology measures distance by calculating the time delay between the emission and reception of a pulse of infrared light. The infra red light returns after reflecting off the surface of the target (e.g. in terrain feature mapping, the light reflects off the Earth's surface). LIDAR can operate in either profiling or scanning mode to illuminate the terrain under study.

LIDAR, in combination with GPS and Inertial Navigational System (INS) data, allows for highly accurate determination of altitude and position for aircraft, missiles, and other weapons and reconnaissance systems.

In addition to military and intelligence applications, LIDAR has been used to map ice flows and monitor storm erosion damage to beaches.

#### ■ FURTHER READING :

##### PERIODICALS:

Harney, R. C. "Physics and Technology of Coherent Infra-red Radar." *Proceedings of the SPIE* Vol. 300 (1981).

Wertner, C., and Bilbro, J. "Coherent Laser Radar: Technology and Applications." *Proceedings of the SPIE* Vol. 1181 (1989).

##### SEE ALSO

*Mapping Technology*  
*Unmanned Aerial Vehicles (UAVs)*

## Lipstick Pistol.

SEE *Assassination weapons, Mechanical.*

## Lock-Picking

Lock-picking is an ability possessed primarily by locksmiths and by persons involved in intelligence or detective work for which secrecy is a necessity. Requiring a high degree of reasoning power and mechanical dexterity, lock-picking even has its amateur enthusiasts who simply enjoy the challenge. The tools of the trade can involve an amazing array of devices, but most are variations on a simple pick mechanism that a skilled and patient practitioner can replicate even with a paper clip.

**Basic technique.** One of the simplest types of lock to pick is known as a pin-and-tumbler design. This lock uses a row of pins, divided into pairs, which rest in a row of shafts running perpendicular to the lock's main cylinder plug and its housing mechanism. Insertion of the right key forces

the top and bottom pins apart at just the right distance so that all of the upper pins rest in the outer housing and all of the lower pins rest in the plug. At that point, no pins bind the plug to the housing, meaning that the cylinder can be turned freely, releasing the bolt that holds the locking mechanism in place.

To open such a lock without a key, one needs a long, thin piece of metal with a curved end (a pick), which can be inserted carefully inside the lock as one would a key. Moving with finesse, it is possible to adjust all the pins into place so that the cylinder can be turned as though the key had been used. Or one can apply a sloppier variation, known as raking, in which a pick is inserted and pulled out quickly while the cylinder is turned with a tension wrench such as a flathead screwdriver.

**Tools.** Experienced lock-pickers use a wide array of tools. They are likely to go to work using an entire tool kit with picks, "rakes" (picks for raking a lock), and tension wrenches, all of which are small enough that a basic lock-picking kit could fit into a pocket. To be equipped for a greater range of eventualities, a lock-picker may use a kit that includes other tools, such as a burglar alarm evasion kit, a key-impression kit (for making a key based on impressions that a lock makes on a key blank), a key-pattern device (for copying old-fashioned warded keys, made to fit into lever locks), files, and other items.

Even more sophisticated is an electric lock-opening device, which is used in tandem with a pick to move the pins into the proper position. Additionally, a lockpick gun can be used to open most pin-tumbler mechanisms. By squeezing the trigger, one strikes the pins with the pick, after which a tension wrench is applied to turn the lock cylinder.

There are other varieties of techniques and tools, just as there are variations in lock design, such as the wafer-tumbler lock, in which tumblers in the shape of wafers take the place of pins. Most aspects of lock-picking are simple in concept, but far from easy in application. Good locksmiths are almost always good lock-pickers, and the reverse is almost as true: a talented lock-picker, for instance, should be able to reconfigure a lock to fit a particular key, a skill that would obviously be of enormous advantage to an intelligence officer in a covert operation.

#### ■ FURTHER READING :

##### BOOKS:

Macaulay, David, with Neil Ardley. *The New Way Things Work*. Boston: Houghton Mifflin, 1998.

Melton, H. Keith. *The Ultimate Spy Book*. New York: DK Publishing, 1996.

Phillips, Bill. *The Complete Book of Locks and Locksmithing*. New York: McGraw-Hill, 1995.

Roper, C. A. *The Complete Book of Locks and Locksmithing*. Blue Ridge Summit, PA: Tab Books, 1983.

Sloane, Eugene A. *The Complete Book of Locks, Keys, Burglar and Smoke Alarms, and Other Security Devices*. New York: Morrow, 1977.

**ELECTRONIC:**

Harris, Tom, and Marshall Brain. How Lock Picking Works. Howstuffworks.com. <<http://home.howstuffworks.com/lock-picking.htm>> (April 5, 2003).

**SEE ALSO**

- Black Ops*
- Covert Operations*
- Locks and Keys*
- Watergate*

---

## Locks and Keys

---

Locks can be either mechanical or electronic, the latter being a modern variation for which a specific numeric code is required to release the locking mechanism. Much more common is a mechanical lock, opened by purely physical means. Locks do not have an independent existence; they must lock something or someone in or out, and they must have a key. The key is based on principles that go back to ancient times, using one of the most rudimentary types of machine known to humankind: the inclined plane.

**Historical background.** In the history of physics and technology, there are three simple machines: the lever, the inclined plane, and the hydraulic press. The last of these only came into existence during the 1600s, but the first two date to a time before the dawn of civilization. The simplest form of inclined plane is a ramp, which makes it possible to move an object across a vertical distance with a smaller amount of exertion than would be required to lift it straight upward. Other modifications of the inclined plane are wedges, knives, axes, screws, corkscrews, and a key and lock mechanism.

The earliest locks date back to ancient Egypt, and even the more modern variations on lock design that developed in the wake of industrialization still harken back to the design used in the pharaohs' palaces. For example, American locksmith and inventor Linus Yale, Jr., whose name remains an important one in the lock and key industry, based his cylinder lock in the 1860s on the Egyptian design. The latter consisted of a wooden housing containing wooden pegs of varying length, fitted into holes bored into the top of a wooden bolt. Only when a long wooden

key with pegs of specific lengths was inserted into the bolt could it be opened.

**Basic workings of a lock.** Modern locks and keys are made of steel rather than wood, but otherwise the design is not remarkably different from that used to lock doors thousands of years ago. Inside a modern mechanical lock is a row of pins, usually five in number. Each pin has its own cylinder, and when the lock is locked, they hold together two pieces of metal rather as the "teeth" of a belt hold together two sections of a piece of leather. The pins are of varying length, meaning that in order to open the lock, it is necessary to raise them all together so that the bottoms are in alignment.

The solution to this problem is, quite literally, a key, whose serrated edge is actually a row of inclined planes fitted to the configuration of pins inside the lock. The notches on the key are made to push the pins upward just the right amount for each pin, so as to force them all into their respective cylinders and separate the two blocks from one another. The shape of the notches is such that the key can be withdrawn from the lock after use, at which point springs push the pins back downward into their original place.

**Mechanical and electronic variations.** A variation on this model is Yale's cylinder lock. In this design, the pins are lined up along a larger metal cylinder, which they hold in place inside a cylindrical housing. Inserting the proper key raises the pins and frees the cylinder so that, when it is turned, it rotates and draws back a cam that holds a bolt in place. The bolt is spring-loaded, such that when the key is withdrawn, the spring pushes the bolt back into place, turning the cylinder back to its original position and making it possible to withdraw the key.

There are other variations on the mechanical lock, most notably the old-fashioned lever lock, but the basic principle is the same. By contrast, an electronic lock requires the use of a keypad and a numeric code. The user enters a code, which the machine interprets as a series of binary (on-off) electric pulses. These pulses are bits in a number sequence, which are read by a computer chip. Assuming the sequence matches the one encoded on the chip, the latter sends out an electric signal that opens a mechanical bolt holding the lock in place.

**■ FURTHER READING:**

**BOOKS:**

- Macaulay, David, with Neil Ardley. *The New Way Things Work*. Boston: Houghton Mifflin, 1998.
- Phillips, Bill. *The Complete Book of Locks and Locksmithing*. New York: McGraw-Hill, 1995.

Roper, C. A. *The Complete Book of Locks and Locksmithing*. Blue Ridge Summit, PA: Tab Books, 1983.

Sloane, Eugene A. *The Complete Book of Locks, Keys, Burglar and Smoke Alarms, and Other Security Devices*. New York: Morrow, 1977.

#### SEE ALSO

*Black Ops*  
*Covert Operations*  
*Lock-Picking*

## Looking Glass

Looking Glass is the nickname for the Airborne Command Post, which was implemented by the U.S. Strategic Air Command (SAC) during the Cold War to ensure that operations would continue in the event that the primary strategic command centers were rendered unusable. The name "Looking Glass" derives from the fact that the aircraft used are equipped to fulfill, or "mirror" all functions normally performed on the ground. In the initial phase of the mission, anticipating possible military aggression by the Soviet Union, SAC had an EC-135 aircraft aloft 24 hours a day, seven days a week. After 1990, as that threat seemed to subside, the continuous flights were discontinued. However, the Looking Glass mission continues with a fleet of highly sophisticated aircraft that may be launched as needed.

**The birth of Looking Glass.** Whereas many people in the second half of the twentieth century envisioned scenarios of global annihilation through nuclear warfare, the U.S. military believed that a nuclear war would actually be more limited and that the Soviets would seek first to neutralize American defensive power. Most command and control centers had been placed, therefore, far from large population centers; few were as important as SAC, located in Offutt, Nebraska.

If the Soviets did decide to attack the United States, wisdom suggested they would send their bombers over the North Pole, giving the U.S. leadership just one hour's notice. With the development of intercontinental ballistic missiles, or ICBMs, in the late 1950s, lead-time was reduced to just 15 minutes. In that span of time, a Soviet ICBM could eliminate the ground center at SAC. It was clear that some response to such a scenario must be developed.

**Looking Glass at work.** This mirror operation of SAC ground control went into service on February 3, 1961, aboard an

EC-135, which had the frame of a Boeing 707 loaded with state-of-the-art communications equipment. Each member of the 24-man crew, composed of personnel from all branches of the armed services, had a specific role. Among these were the positions of airborne launch control officer, emergency actions non-commissioned officer, and force status non-commissioned officer. At the lead was a commander, assisted by an integrated operations plan advisor, who advised the commander regarding the war plans available to the president.

Over the years that followed, Looking Glass pursued its mission, one as grim—based as it was on a doomsday scenario—as it was necessary. During that time, one Looking Glass craft was always in the air, night and day, while at least one more waited on the ground, fully manned and prepared to take over. Over the course of 29 years of nonstop flying, Looking Glass crews accumulated more than 281,000 accident-free hours aloft.

**Post Cold-War changes.** On July 24, 1990, with the Berlin Wall a memory and the Soviet Union fast receding from the world stage, Looking Glass ended its continuous airborne alert mission. Thenceforth, the system would make use of fewer planes, which operated on an alert status—ready to fly at a moment's notice, but not necessarily aloft at all times.

Further changes followed. In 1992, SAC was disestablished and replaced by the United States Strategic Command (USSTRATCOM), and Looking Glass became a joint military operation. Then in 1998 EC-135 planes were retired and replaced by the newer E-6B, known as the "Take Charge and Move Out" (TACAMO) aircraft. Also based on the 707 airframe, the E-6B accommodated a crew of 15 or more.

#### ■ FURTHER READING:

##### PERIODICALS:

Healy, Melissa. "Doomsday Plane's Round-the-Clock Flights Called Off." *Los Angeles Times*. (July 28, 1990): 2.  
"Looking Glass Gets a Rest at Last." *Chicago Tribune*. (July 29, 1990): 2.

##### ELECTRONIC:

E-6B Airborne Command Post (ABNCP). U.S. Strategic Command. <<http://www.stratcom.af.mil/factsheetshtml/ABNCP.htm>> (April 3, 2003).  
EC-135, Looking Glass. Federation of American Scientists. <<http://www.fas.org/nuke/guide/usa/c31i/ec-135.htm>> (April 3, 2003).  
Looking Glass. Nebraska Studies.org. <[http://www.nebraskastudies.org/0900/stories/0901\\_0124.html](http://www.nebraskastudies.org/0900/stories/0901_0124.html)> (April 3, 2003).

#### SEE ALSO

*Cold War (1950–1972)*



The last of the EC-135 planes used for the Looking Glass mission from 1961 to 1998 taxis to its retirement ceremony at Offutt Air Force Base in Nebraska. In 1998, the Looking Glass mission began using the newer E-6B plane. AP/WIDE WORLD PHOTOS.

*Nuclear Weapons*  
*USSTRATCOM (United States Strategic Command)*

## “Loose Nukes.”

SEE *Russian Nuclear Materials, Security Issues.*

---

## Lord Haw-Haw

---

■ ADRIENNE WILMOTH LERNER

Lord Haw-Haw was the nickname of Nazi propagandist and broadcaster William Joyce. During World War II, Joyce broadcast a well-known English-language propaganda show from Berlin, often taunting Allied forces. Though never calling himself Lord Haw-Haw on air, he became infamous among Allied combat troops and British citizens.

Joyce was born in Brooklyn, New York, the son of an Irish father and English mother. His family returned to England when he was an infant. As an adult, Joyce joined several radical political organizations, including the British Fascisti. He wrote a series of articles for several extremist newspapers and gained a reputation as a skilled

propagandist. In 1934, he served as the Director of Propaganda for the British Union of Fascists. While serving the political organization, Joyce donned full Blackshirt uniform and engaged in a number of street fights with protestors, earning his trade mark facial scar in one scuffle.

As Joyce gained power in the organization, he became more radical. He used his position as a platform for his deeply anti-Semitic views, blaming most of the era’s political and social ills on “Jewish communists.” He formed his own political party, the British National Socialist League, in 1937. The party proclaimed brotherhood with the Nazi party in Germany and championed similar causes.

Before the war, Joyce did not attempt to disguise his admiration for Adolph Hitler and Nazi policies. On August 26, 1939, Joyce fled to Berlin. He narrowly escaped arrest in Britain under a law that mandated the detention of Nazi sympathizers and political activists. Shortly after arriving in Berlin, Joyce formally joined the Nazi Party. He took a job working on an anti-Allied propagandist radio show.

British journalists were quick to dismiss Joyce’s broadcasts and portrayed him a mere stooge. He was dubbed “Lord Haw-Haw” because of his distinct nasal drawl. Listening to Lord Haw-Haw’s show was technically prohibited in Britain under a ban on enemy radio, but the show was popular on the British home front. The program drew strong denunciation, but many simply laughed at its absurdity and obviously propagandistic content. On a few occasions, the program managed to frighten listeners with discussions of German saboteurs in Britain and with accurate details of British towns, such as descriptions of belfries and landmarks.



At the war's end, Joyce fled Berlin and broadcast his final shows from Hamburg. When allied forces moved to occupy the city, Joyce retreated to nearby Flensburg and was captured. He was shot in the leg in the process of trying to escape into a patch of woods. Joyce was turned over to British authorities and detained until he was flown back to Britain as a prisoner.

The British government passed a new Treason Act of 1945 in order to prosecute citizens who seriously impeded or compromised the British war effort. The media attention surrounding Joyce's radio program and capture, as well as their portrayal of Joyce as a possible spy, encouraged the government to charge Joyce with treason under the new act. Although the courts could not substantiate charges of espionage, they did convict Joyce of treason based on his broadcasts and voluntary association and cooperation with Nazi officials. Joyce was sentenced to death by gallows and executed on January 3, 1946.

#### ■ FURTHER READING:

##### BOOKS:

Martland, Peter. *Lord Haw-Haw: The English Voice of Nazi Germany*. Barnsley, South Yorkshire: Pen & Sword Books, 2003.

##### SEE ALSO

*Tokyo Rose  
Propaganda, Uses and Psychology*

## Lord's Resistance Army (LRA)

Founded in 1989, the Lord's Resistance Army (LRA) was the successor to the Holy Spirit Movement. The LRA seeks to overthrow the incumbent Ugandan government and replace it with a regime that will implement the group's brand of Christianity. The LRA frequently kidnaps and kills local Ugandan civilians in order to discourage foreign investment and precipitate a crisis in Uganda.

The LRA is estimated to have 2,000 members who operate in northern Uganda and southern Sudan. The LRA has been supported by the government of Sudan.

#### ■ FURTHER READING:

##### ELECTRONIC:

CDI (Center for Defense Information), Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <<http://www.cdi.org/terrorism/terrorist.cfm>> (April 17, 2003).

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001." Annual Report: On the Record Briefing. May 21, 2002 <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

##### SEE ALSO

*Terrorism, Philosophical and Ideological Origins  
Terrorist and Para-State Organizations  
Terrorist Organization List, United States  
Terrorist Organizations, Freezing of Assets*

## Los Alamos National Laboratory

#### ■ K. LEE LERNER

Los Alamos National Laboratory (LANL), located near Sante Fe, New Mexico, is operated by the University of California for the National Nuclear Security Administration (NNSA, a component of the United States Department of Energy).

Founded in 1942, LANL was initially staffed by a team of physicists under the direction of J. Robert Oppenheimer to work on the development of an atomic bomb as part of the Manhattan Project. LANL is now a major research facility with approximately 50 operational laboratories. LANL also hosts supercomputing facilities that support both on-site and off-site research programs. Research at LANL brings scientists from a variety of disciplines to work on military and non-military related projects. LANL scientists have developed a number of technologies related to national security interests.

Research at LANL has broadened from its initial emphasis on physics and engineering into biotechnology related projects. LANL scientists participated in the development of the human genome map. Research programs also develop and improve an array of detection devices—including bio-detectors—that are used by intelligence and law enforcement agencies to detect the presence of nuclear, biological, or chemical weapons, or weapons related materials. LANL engineers develop and provide handheld radiation and isotope identifiers. LANL also provides other agencies technical advice and training in detector use.

LANL personnel directly and indirectly support DOE Nuclear Emergency Support Team (NEST) operations that



A program director of the nuclear weapons computing department at Los Alamos National Laboratory stands among the many components of a supercomputer called Blue Mountain at the lab in Los Alamos, New Mexico. AP/WIDE WORLD PHOTOS.

are designed to provide rapid response to accidents or terrorist use of radiological materials. NEST teams would be a critical part of first response operations in the event of a "dirty bomb" attack (i.e., an attack using a non-nuclear explosion to disperse radioactive materials).

Nuclear detection technologies developed as a part of NNSA's Materials Protection, Control and Accounting (MPC&A) program are used by International Atomic Energy Agency (IAEA) inspectors and some foreign countries (e.g., the Russian Federation) to enhance security of nuclear materials and to deter the unintentional transfer of nuclear materials and nuclear technology to terrorists or nations seeking to develop nuclear weapons.

Bio-detector technologies include the Biological Aerosol Sentry and Information System (BASIS), designed to warn of airborne biological weapons attacks; Swept Frequency Acoustic Interferometer (SFAI) technologies allow detection of chemicals that may be components of chemical weapons. BASIS detectors were used at the 2002 Winter Olympics in Utah. SFAI detectors, termed "stand-off acoustic identification" detectors provide inspection teams with remote sensing capabilities that enhance safe inspection of packages because traces of chemical elements can often be detected without unsealing containers or opening packages.

LANL's powerful supercomputers allow epidemiologists and biohazard specialists to develop detailed modeling programs to forecast dispersal patterns of airborne toxins.

Not all research programs have direct security applications; some hold the potential for broad engineering applications in industry. For example, LANL scientists have developed tape capable of conducting electricity with very low resistance, and computer specialists have developed software capable of improving regulation of engine ignition systems to promote greater fuel efficiency. LANL personnel often work in conjunction with industry contractors in industrial partnership programs. Other LANL programs support medical research; for example, laboratory teams have assembled a vast virus database that is used around the world to facilitate research into a potential AIDS vaccine.

As one of three NNSA national laboratories, LANL scientists have contributed to a number of research projects designed to support arms control and counterterrorism technologies. Following the September 11, 2001, terrorist attacks on the United States, LANL's Center for Homeland Security assumed the role of coordinating work on homeland security and counterterrorism technologies.

In conjunction with Sandia National Laboratory scientists, LANL engineers developed the National Infrastructure Simulation and Analysis Center (NISAC) that allows officials to create and test response strategies. Threat analysis and warning technologies provide intelligence and law enforcement agencies enhanced capabilities to deter smuggling and other terrorist-related activities. LANL research programs are also attempting to improve INS (Immigration & Naturalization Service) regulation of border activity by improving automated entry/exit systems. One such program—GENetic Imagery Exploitation (GENIE)—is designed to improve biometric and feature-extraction analysis.

#### ■ FURTHER READING :

##### ELECTRONIC:

Los Alamos National Laboratory. <<http://www.lanl.gov/worldview/>> (March 23, 2003).

United States Department of Energy, Office of Science. National Laboratories and User Facilities. <[http://www.sc.doe.gov/Sub/Organization/Map/national\\_labs\\_and\\_userfacilities.htm](http://www.sc.doe.gov/Sub/Organization/Map/national_labs_and_userfacilities.htm)> (March 23, 2003).

United States Department of Homeland Security. Research & Technology. <<http://www.dhs.gov/dhspublic/display?theme=27&content=374>> (March 23, 2003).

University of California. Department of Energy National Laboratories. <<http://www.universityofcalifornia.edu/labs/>>(March 22, 2003).

##### SEE ALSO

*Argonne National Laboratory*  
*Brookhaven National Laboratory*  
*DOE (United States Department of Energy)*  
*Environmental Measurements Laboratory*  
*Lawrence Berkeley National Laboratory*  
*Lawrence Livermore National Laboratory (LLNL)*  
*NNSA (United States National Nuclear Security Administration)*  
*Oak Ridge National Laboratory (ORNL)*  
*Pacific Northwest National Laboratory*  
*Plum Island Animal Disease Center*  
*Sandia National Laboratories*

## Loyalist Volunteer Force (LVF)

The Loyalist Volunteer Force (LVF) is an extreme loyalist group formed in 1996 as a faction of the mainstream

loyalist Ulster Volunteer Force (UVF), though it did not emerge publicly until February, 1997. The LVF is composed largely of UVF hardliners who have sought to prevent a political settlement with Irish nationalists in Northern Ireland by attacking Catholic politicians, civilians, and Protestant politicians who endorse the Northern Ireland peace process. In October, 2001, the British Government ruled that the LVF had broken the cease-fire it declared in 1998. The LVF decommissioned a small but significant amount of weapons in December, 1998, but it has not repeated this gesture as of May, 2002. LVF participates in bombings, kidnappings, and close-quarter shooting attacks. LVF bombs often have contained Powergel commercial explosives, typical of many loyalist groups. LVF attacks have been particularly vicious: The group has murdered numerous Catholic civilians with no political or terrorist affiliations, including, in July 1997, an 18-year-old Catholic girl who had a Protestant boyfriend. The terrorists also have conducted successful attacks against Irish targets in Irish border towns. In 2000 and 2001, the LVF also engaged in a violent feud with other loyalists in which several individuals were killed.

LVF has approximately 150 activists who operate in Northern Ireland and Ireland.

#### ■ FURTHER READING :

##### ELECTRONIC:

CDI (Center for Defense Information), Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <<http://www.cdi.org/terrorism/terrorist.cfm>> (April 17, 2003).

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001." Annual Report: On the Record Briefing. May 21, 2002 <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17,2003).

U.S. Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

##### SEE ALSO

*Terrorism, Philosophical and Ideological Origins*  
*Terrorist and Para-State Organizations*  
*Terrorist Organization List, United States*  
*Terrorist Organizations, Freezing of Assets*

*This page intentionally left blank*



## MAD (Mutually Assured Destruction).

SEE *Strategic Defense Initiative and National Missile Defense*.

## Mad Man Theory.

SEE *Cold War (1950–1972)*.

## Magic Chips (Micro Array of Gel-Immobilized Compounds).

SEE *Argonne National Laboratory*.

persons who were infected by the anthrax bacterium died from the disease. As a direct result of this, the USPS developed an Emergency Preparedness Plan with the goal of protecting USPS employees and customers from future bioterrorism attacks. The plan is composed of six initiatives:

- Prevention—reducing the risk that the mail could be used as a vehicle for bioterrorism
- Protection and health-risk reduction—reducing the risk that USPS employees and customers could be exposed to biological weapons and preventing contaminated mail from contaminating other mail
- Detection and identification—detection and identification of biological weapons as early in the mail stream as possible
- Intervention—routine decontamination of mail as a precautionary measure
- Decontamination—elimination of known biological weapons in the mail
- Investigation—enhancement of criminal investigation methods

Mail sanitization applies to the intervention and decontamination initiatives. Achieving mail safety is no small undertaking when one considers the complexity of the USPS system and volume of mail that is processed. The postal service handles nearly 680 million pieces of mail each day. This mail is primarily letters, “flats” such as catalogs and magazines, and packages. Mail enters the USPS system in many different ways including street collection boxes, post offices, personal mailboxes, and business mail entry units. The USPS has about 300 processing and distribution centers that manage outgoing mail. The computer-controlled sorting equipment and data processing systems located at these centers distribute mail to its destination. Mail is moved from processing and distribution centers to final destination processing centers by ground, rail, or air transportation. Once at a final destination processing center, mail is then sorted and distributed to the recipients.

---

## Mail Sanitization

---

■ BELINDA ROWLAND

Mail sanitization is the process in which mail is decontaminated by exposure to radiation, high pressure, or gases. Microorganisms, such as the bacterium that causes anthrax, cannot survive these conditions. The process of mail sanitization can be applied as a precautionary measure to kill microorganisms that may be contained in the mail or to sterilize mail that is known to be contaminated.

Shortly after the September 11, 2001, terrorist attacks, the United States Postal Service (USPS) was the vehicle for bioterrorism attacks on the American people. Mail containing the anthrax bacterium was detected. Five

## Methods to Sanitize Mail

The USPS is studying several different methods of decontamination to find one (or more) that can effectively sanitize mail. To be useful in mail sanitization, the decontamination method must thoroughly penetrate letters, flats, and packages but not damage the mail in any way. As of late 2002, irradiation was the only acceptable method for decontaminating mail. The addition of a sanitization step to the USPS mail system may slow down the mail delivery rate.

**Ionizing radiation.** Ionizing radiation kills bacteria. The energy from ionizing radiation is absorbed by molecules, breaking chemical bonds and thus destroying chemical structures. Reactive chemicals (ions and free radicals) that are produced by this process cause even further damage. This results in significant damage to the DNA and proteins of bacteria and causes them to die.

The USPS is considering three sources of ionizing radiation as candidates for mail sanitization: x rays, gamma rays, and electron beams. All three are used to sterilize medical equipment and to kill microorganisms in food to prevent spoilage. They each can kill the anthrax bacteria. Radiation can easily penetrate and sanitize most types of mail, however, it may damage film, electronics, and live objects such as seeds.

X rays are a type of high-energy electromagnetic radiation. X-ray particles, or photons, are generated when electron-dense materials are bombarded by high-energy electrons. X rays have a high-energy content and can penetrate most objects.

Gamma rays are another type of high-energy electromagnetic radiation. Gamma rays are released by decaying radioactive compounds such as cesium 137 or cobalt 60.

An electron beam, or e-beam, is a stream of electrons that is propelled by a high accelerating voltage. The energy content of the e-beam is determined by the accelerating voltage and is lower than both x rays and gamma rays.

Of the three ionizing radiation sources, e-beam technology is the safest and most readily adaptable system for mail sanitization. In 2001, the USPS bought eight e-beam machines and planned to install them in Washington D.C. and the New York and New Jersey area. The e-beam machine requires high power and chilled water and must be contained by a structure with 10 to 15 foot-thick concrete walls and a six foot-thick concrete ceiling. As of late 2002, e-beam technology has been used to sanitize incoming federal government mail only.

**Non-ionizing radiation.** Types of non-ionizing radiation that have been used for sterilization are ultraviolet (UV) light and microwaves. Both are effective at killing microorganisms, but in different ways.

UV light radiation damages DNA by causing DNA strand breaks and binding DNA bases together (thymine dimers). Bacteria with damaged DNA cannot reproduce or survive. UV light radiation cannot penetrate objects and is used to sterilize surfaces and air only. In addition, some microorganisms are resistant to the effects of UV radiation. Therefore, UV radiation is an unacceptable method to sanitize mail.

Microwave radiation is a low energy non-ionizing radiation. The energy in microwaves is transferred to water molecules in microorganisms. The water molecules heat up and the heat is transferred to surrounding molecules, thereby damaging and ultimately killing the microorganism. Microwave radiation sanitization has shortcomings. Most importantly, it is difficult to control the heating effects and it is common to have "hot spots" and "cold spots." Also, the water content of dormant bacterial cells (spores) is low, so microwave radiation may not destroy them. Microwave radiation would be ineffective for mail sanitization.

**Ultra-high-pressure sterilization.** Ultra-high-pressure (UHP) sterilization is accomplished by applying a pressure of almost 100,000 psi, which causes physical changes to DNA and proteins. The resulting cellular damage kills the microorganisms. Without added heat, UHP sterilization techniques may be less effective against bacterial spores than against growing bacterial cells.

UHP sterilization is being developed for the food industry and has been shown to be effective on both solid and liquid foods. The UHP sterilization cycle time can be less than 30 minutes and the process is non-destructive to the object being sterilized. This method could be applied to mail as a sanitization method, however, a UHP sterilization system for mail will not be available for several years.

**Gaseous treatment.** Certain gases have anti-microbial properties and are used for disinfection and sterilization. The USPS has identified chlorine dioxide, ethylene oxide, methyl bromide, and ozone as candidates for gaseous sanitization.

- Chlorine dioxide: an oxidizer that disrupts proteins and protein synthesis. It was used to disinfect an office building that was contaminated with anthrax spores.
- Ethylene oxide: an alkylating agent that damages proteins, leading to bacterial or viral death. It is used to sterilize medical equipment.
- Methyl bromide: a toxic pesticide that has been used to fumigate large buildings. It is an ozone-depleting chemical and will not be used after 2006.
- Ozone: an oxidizing agent used to disinfect water and decontaminate unoccupied spaces. Its effect on spores is variable depending upon the specific bacterial strain.

Large amounts of gas would be needed to sterilize mail and it is not evident that gases can kill microorganisms within sealed letters, flats, and packages. Gaseous sterilization of mail is not currently a viable option for mail sanitization.

#### ■ FURTHER READING :

##### PERIODICALS:

"Months After Anthrax Scare, Mail-Safety Goals are Unmet." *USA Today*. (August 29, 2002): 12a.

"USPS Builds to Sterilize Mail." *Engineering News-Record* no. 247 (November 26, 2001): 11.

##### ELECTRONIC:

United States Postal Service. <<http://www.usps.com/welcome.htm>>(December 14, 2002).

##### SEE ALSO

*Anthrax, Terrorist Use as a Biological Weapon*  
*Bioterrorism, Protective Measures*  
*Decontamination Methods*  
*Postal Security*  
*Postal Service (USPS), United States*  
*Radiation, Biological Damage*  
*September 11 Terrorist Attacks on the United States*

## Malicious Data

Malicious data is data that, when introduced to a computer—usually by an operator unaware that he or she is doing so—will cause the computer to perform actions undesirable to the computer's owner. It often takes the form of input to a computer application such as a word-processing or spreadsheet program. It is thus distinguished from a malicious program such as a computer virus, compared to which malicious data is perhaps even more stealthy.

An example of malicious data at work is the Melissa "virus," which spread through the e-mail systems of the world on March 26, 1999. Though the media called Melissa a virus, this was a misnomer; rather, it was a case of malicious data wedded to a macro virus, or a virus that works by setting in motion an automatic sequence of actions within a software application. Melissa did not damage computers themselves, yet it produced a result undesirable to anyone but its creator. By taking advantage of a feature built into the Microsoft Word program, it sent itself to the first 50 addresses in the user's Outlook Express, an e-mail program also produced by Microsoft. Melissa, for which computer programmer David L. Smith was eventually charged, caused \$80 million worth of damage, primarily in the form of lost productivity resulting from the shutdown of overloaded mailboxes.

In practice, malicious data is much like a malicious program, yet it is difficult to protect against malicious data using the methods typically used to circumvent malicious programs, such as file access control, firewalls, and the like. Malicious data has been used not simply for pranks such as Smith's, but to transfer funds out of the operator's financial accounts, and into those of the perpetrator. In this crime, the operator him- or herself is a participant, albeit an unwitting and unwilling one.

#### ■ FURTHER READING :

##### BOOKS:

Gelman, Robert B., and Stanton McCandlish. *Protecting Yourself Online: The Definitive Resource on Safety, Freedom, and Privacy in Cyberspace*. New York: HarperEdge, 1998.

Schneier, Bruce. *Secrets and Lies: Digital Security in a Networked World*. New York: John Wiley, 2000.

Schwartz, Winn. *Cybershock: Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorists, and Weapons of Mass Disruption*. New York: Thunder's Mouth Press, 2000.

##### PERIODICALS:

Mitchell, Russ, Richard Folkers, and Susan Gregory. "Why Melissa Is So Scary." *U.S. News & World Report*. (April 12, 1999): 34–36.

##### ELECTRONIC:

Sibert, W. Olin. Malicious Data and Computer Security. <<http://home.earthlink.net/~wolfboy/ARCHIVE/GenSecure/maldata.htm>> (April 3, 2003).

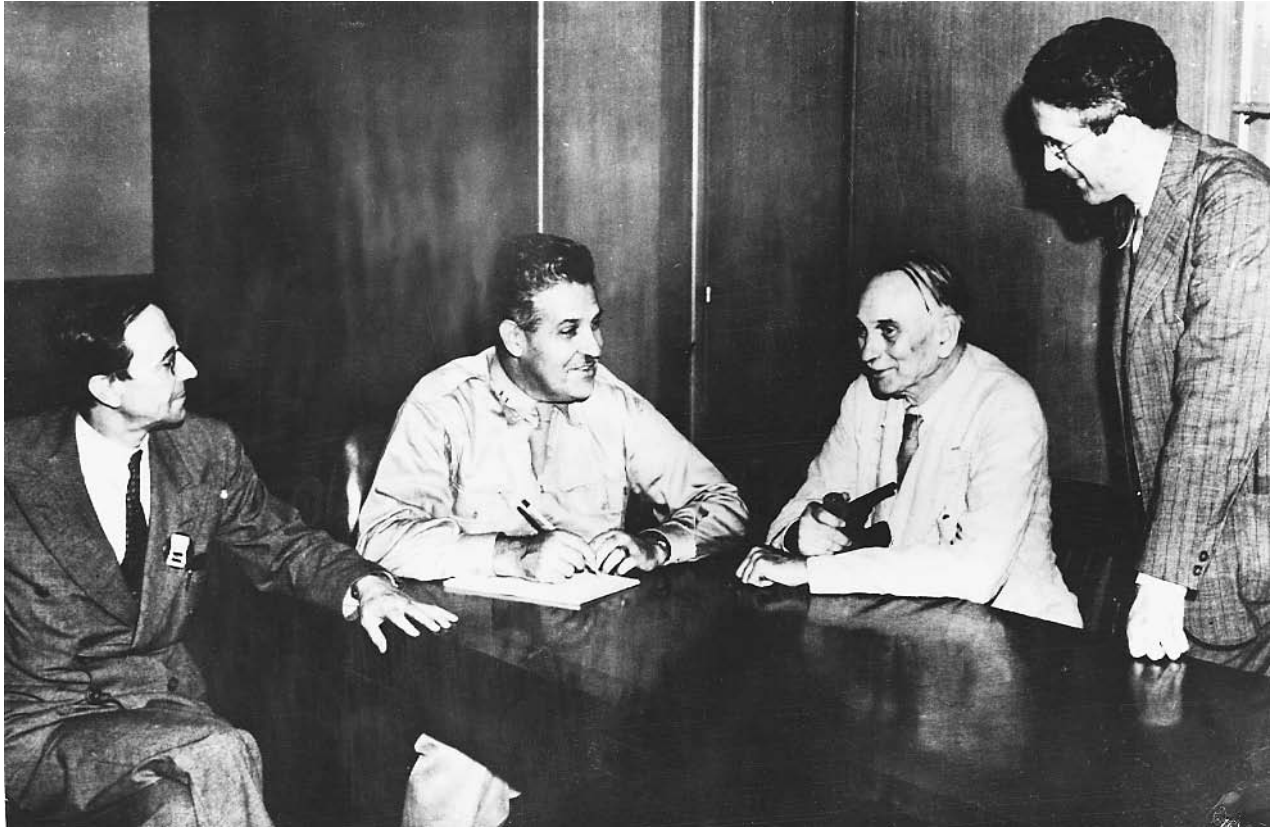
##### SEE ALSO

*Computer Hackers*  
*Computer Software security*  
*Computer Virus*  
*Infrastructure Protection Center (NIPC), United States National*

## Manhattan Project

#### ■ BRENDA WILMOTH LERNER

The Manhattan Project was an epic, secret, wartime effort to design and build the world's first nuclear weapon. Commanding the efforts of the world's greatest physicists and mathematicians during World War II, the \$20 billion project resulted in the production of the first uranium and plutonium bombs. The American quest for nuclear explosives was driven by the fear that Hitler's Germany would invent them first and thereby gain a decisive military advantage. The monumental project took less than four years, and encompassed construction of vast facilities in Oak Ridge, Tennessee, and Hanford, Washington, that



Brigadier General Leslie Groves (second from left), shown in conversation with Manhattan project scientists Sir James Chadwick (left), Dr. Richard Tolman (second from right), and Dr. H. D. Smyth. ©HULTON-DEUTSCH COLLECTION/CORBIS.

were used for the purpose of obtaining sufficient quantities of the isotopes uranium-235 and plutonium-239, necessary to produce the fission chain reaction, which released the bombs' destructive energy. After a successful test in Alamogordo, New Mexico, the United States exploded a nuclear bomb on the Japanese city of Hiroshima on August 6, 1945. Three days later another bomb was dropped on the Japanese city of Nagasaki, and spurred the Japanese surrender that ended World War II.

In the 1930s and early 1940s, fundamental discoveries regarding the neutron and atomic physics allowed for the possibility of induced nuclear chain reactions. Danish physicist Neils Bohr's (1885–1962) compound nucleus theory, for example, laid the foundation for the theoretical exploration of fission, the process whereby the central part of an atom, the nucleus, absorbs a neutron, then breaks into two equal fragments. In certain elements, such as plutonium-239, the fragments release other neutrons which quickly break up more atoms, creating a chain reaction that releases large amounts of heat and radiation.

Hungarian physicist Leo Szilard (1898–1964) conceived the idea of the nuclear chain reaction in 1933, and immediately became concerned that, if practical, nuclear energy could be used to make weapons of war. Szilard, who fled Nazi persecution first in his native Hungary, then again in

Germany, conveyed his concerns to his friend and contemporary, noted physicist Albert Einstein (1879–1955). In 1939, the two scientists drafted a letter (addressed from Einstein) warning United States President Franklin D. Roosevelt of the plausibility of nuclear weapons, and of German experimentation with uranium and fission. In December, 1941, after the Japanese attack at Pearl Harbor and the United States' entry into the war, Roosevelt ordered a secret United States project to investigate the potential development of atomic weapons. The Army Corps of Engineers took over and in 1942 consolidated various atomic research projects into the intentionally misnamed Manhattan Engineering District (now commonly known as the Manhattan Project), which was placed under the command of Army Brigadier General Leslie Richard Groves.

Groves recruited American physicist Robert Oppenheimer (1904–1967) to be the scientific director for the Manhattan Project. Security concerns required the development of a central laboratory for physics weapon research in Los Alamos, New Mexico. Oppenheimer's leadership attracted many top young scientists, including American physicist Richard Feynman (1918–1988), who joined the Manhattan Project while still a graduate student. Feynman and his mentor Hans Bethe (1906–) calculated the critical mass fissionable material necessary to begin a chain reaction.



Fuel for the nuclear reaction was a primary concern. At the outset, the only materials seemingly satisfactory for sustaining an explosive chain reaction were either U-235 (derived from U-238) or P-239 (an isotope of the yet unsynthesized element plutonium). Additional requirements included an abundant supply of heavy water (e.g., deuterium and tritium). At Oak Ridge, the process of gaseous diffusion was used to extract the U-235 isotope from uranium ore. At Hanford, production of P-239 was eventually made possible by leaving plutonium-238 in a nuclear reactor for an extended period of time.

In 1942, Italian physicist Enrico Fermi (1901–1954) supervised the first controlled sustained chain reaction at the University of Chicago. Underneath the university football stadium, in modified squash courts, Fermi and his team assembled a lattice of 57 layers of uranium metal and uranium oxide embedded in graphite blocks to create the first reactor pile.

The Manhattan Project eventually produced four bombs. Little Boy, the code name for the uranium bomb, utilized explosives to crash pieces of uranium together to begin an explosive chain reaction. Fat Man, the code name for the plutonium bomb, was more difficult to design. It required a neutron-emitting source to initiate a chain reaction within a series of concentric nested spheres. The outermost shell was an explosive lens system surrounding a pusher/neutron absorber shell designed to reduce the effect of Taylor waves, the rapid drop in pressure that occurs behind a detonation front and could interfere with an implosion. The next nested sphere was a uranium tamper/reflector shell containing a plutonium pit and beryllium neutron initiator. The spheres were designed to implode, causing the plutonium to fuse, reach critical mass, then start the reaction.

The simple design of the uranium bomb left scientists confident of its success, but the complicated implosion trigger required by the plutonium bomb raised engineering concerns about reliability. On July 16, 1945, a plutonium test bomb code named Gadget was detonated in a remote area near Alamogordo, New Mexico. Observed by scientists wearing only welder's glasses and suntan lotion for protection, the test blast (code named Trinity) was more powerful than originally thought, roughly equivalent to 20,000 tons of TNT, and caused total destruction up to one mile from the blast center.

Protecting the secrecy of the Manhattan Project was one of the most complex intelligence and security operations during the war. At the Los Alamos facility, all residents were confined to the project area and surrounding town. Though several leading scientists knew the nature and scope of the entire project, most lab facilities were compartmentalized with various teams working on different project elements. Those who worked in the lab were forbidden to discuss any aspect of the project with friends or relatives. Military security personnel guarded the grounds and monitored communications between research teams. Official communications outside of Los Alamos, especially to the other Manhattan Project sites, were coded

and enciphered. Mail was permitted, but heavily censored. Since the actual location of the Los Alamos facility was secret, all residents used the clandestine address "Box 1663, Santa Fe, New Mexico," for correspondence.

Communities were created around other project sites as well. The government created the towns of Oak Ridge and Hanford, relocating thousands of area residents before beginning construction. The towns, thus secured for facility personnel and their families, placed severe restrictions on civilian activities. In some areas, private telephones and radios were prohibited. Residents were encouraged to use simple pseudonyms outside of the lab. Children did not use their full names in school in Oak Ridge, Tennessee.

Managing several different facilities, spaced nearly two thousand miles apart, raised some significant security challenges. Communication was limited, and incoming and outgoing traffic from facility areas was closely monitored. Security of key documents was a constant concern. The isolated locations of the sites helped to insulate them from enemy espionage. However, the separate locations were also a key security strategy. Breaking the Manhattan Project into various smaller operations prevented jeopardizing the entire project in the event of a nuclear accident. The compartmentalization of such projects remains a common practice.

On August 6, 1945, an American B-29 "Flying Fortress," the *Enola Gay*, dropped the uranium bomb over Hiroshima. Sixty thousand people were killed instantly, and another 200,000 subsequently died as a result of burn and radiation injuries. Three days later, a plutonium bomb was dropped over Nagasaki. Although it missed its actual target by over a mile, the more powerful plutonium bomb killed or injured more than 65,000 people and destroyed half of the city. Ironically, ground zero, the point under the bomb explosion, turned out to be the Mitsubishi Arms Manufacturing Plant, at one time the major military target in Nagasaki. The fourth bomb remained unused.

Many Manhattan Project scientists eventually became advocates of the peaceful use of nuclear power and advocates for nuclear weapons control.

#### ■ FURTHER READING:

##### BOOKS:

Fermi, Rachel, and Esther Samra. *Picturing the Bomb: Photographs from the Secret World of the Manhattan Project*. New York: H. N. Abrams, 1995.

Norris, Richard. *Racing For the Bomb: General Leslie R. Groves, the Manhattan Project's Indispensable Man*. South Royalton, VT: Steerforth Press, 2002.

Rhodes, Richard. *The Making of the Atomic Bomb*. New York: Touchstone, 1995 (reprint).

##### ELECTRONIC:

Los Alamos National Laboratory. Manhattan Project History. "The Italian Navigator Has Landed in the New

World. Secret Race Won with Chicago's Chain Reaction" <<http://www.lanl.gov/worldview/welcome/history.shtml>> (February, 24, 2003).

National Atomic Museum, Albuquerque, New Mexico. "The Manhattan Project." <<http://www.atomicmuseum.com/tour/manhattanproject.cfm>>(February 24, 2003).

#### SEE ALSO

*Heavy Water Technology*  
*Los Alamos National Laboratory*  
*Nuclear Detection Devices*  
*Nuclear Reactors*  
*Nuclear Regulatory Commission (NRC), United States*  
*Nuclear Weapons*  
*Oak Ridge National Laboratory (ORNL)*  
*Quantum Physics: Applications to Espionage, Intelligence, and Security Issues*  
*Weapons of Mass Destruction*

## Mapping Technology

■ WILLIAM C. HANEBERG

Mapping technology is a broad term that describes the equipment and techniques used to prepare, analyze, and distribute maps of all kinds. This can include satellites used to obtain high resolution and multispectral data; software to enhance or classify digital images; global positioning system (GPS) satellites; and geographic information systems (GIS).

Intelligence-related mapping within the United States is largely the responsibility of the National Imagery and Mapping Agency. It was formed in 1996 by consolidating the capabilities of several federal agencies involved with the acquisition and analysis of imagery and other forms of geospatial intelligence. The U.S. Geological Survey, a civilian agency within the Department of the Interior, produces detailed topographic and geologic maps of areas within the United States.

One of the primary uses of mapping technology is to gather data from which maps can be made. Classified images from intelligence satellites and sub-meter resolution images from both government and commercial satellites can be used to obtain information about the civil and military infrastructure of foreign powers without having to set foot in dangerous or restricted areas. Technologies such as interferometric synthetic aperture radar (InSAR) can be used to create digital elevation models (DEMs) depicting the elevation of the Earth's surface and serve as the basis for detailed topographic maps. The Shuttle Radar Topography Mission, flown in February 2000, used specialized InSAR technology to map the elevation of Earth's land surface between 60 degrees north and 56 degrees south latitude. Elevations were measured every arc-second of latitude and longitude, which is equivalent to a spacing of about 30 m. Detailed topographic information

such as that collected by the Shuttle Radar Topography Mission can be used to create topographic maps that are essential to military operations or to depict realistic landscapes in combat training simulators.

Multispectral imagery is created using sensors that respond to different bands within the visible and invisible portions of the electromagnetic spectrum. An image that appears to be a color photograph may actually be a color composite composed of, at minimum, red, blue, and green bands. Hyperspectral images are those in which the spectrum is divided into many narrow bands instead of several broad bands. Multispectral or hyperspectral image processing can be used to make inferences about soil or bedrock type, soil moisture, crop growth, chemical pollution, and other properties. Military or intelligence applications can include the determination of the ground conditions to be encountered by an invasion force or estimation of an enemy's crop production. Domestic applications include monitoring elements of a nation's infrastructure, for example unguarded energy transmission lines that are vital to national security and may present targets to terrorist networks.

The global positioning system (GPS) is a network of 24 satellites orbiting Earth at an altitude of 20,200 m (12.55 mi). Launched and maintained by the United States military, the satellites issue signals that can be decoded by GPS receivers to determine the location of the receiver and the time within several hundred nanoseconds. While it is principally a navigational system, GPS is also an important piece of mapping technology. Scientists, geographers, land surveyors, and others can use GPS to determine with great accuracy the locations of objects to be shown on maps. GPS receivers installed on moving vehicles, for example trucks carrying nuclear materials, allow them to be continuously tracked and maps of their locations updated in real time.

Geographic information system (GIS) software allows users to digitally store, retrieve, analyze, and display maps of all kinds. Maps created using different scales or projections can be adjusted and combined to form new composite maps that answer specific questions. For example, a GIS user can combine a computer model of air pollution dispersion with meteorological and troop location data to simulate the effects of possible chemical weapons attacks in different locations. GIS is likewise useful for homeland security projects such as constructing maps of critical infrastructure, developing emergency response plans, and evaluating the consequences of terrorist attacks.

#### ■ FURTHER READING:

##### BOOKS:

Burrough, P. A., and R. A. McDonnell. *Principles of Geographic Information Systems*, 2nd ed. Oxford: University Press, 1998.

Wilford, G. N. *The Mapmakers*. New York: Knopf, 2000.

**ELECTRONIC:**

National Imagery and Mapping Agency. "NIMA Home." <<http://www.nima.mil/>>(December 9, 2002).

National Imagery and Mapping Agency. "Shuttle Radar Topography Mission Navigation Page." October 11, 2002. <<http://www.nima.mil/srtm/navigation.html>> (December 9, 2002).

Dana, Peter H. "The Global Positioning System." May 1, 2000. <[http://www.colorado.edu/geography/gcraft/notes/gps/gps\\_f.html](http://www.colorado.edu/geography/gcraft/notes/gps/gps_f.html)> (December 9, 2002).

Lawrence Livermore National Laboratory. "GIS Group Home Page." August 24, 2000. <<http://gis.llnl.gov/indexm.html>>(December 9, 2002).

**SEE ALSO**

*Geospatial Imagery*  
*NIMA (National Imagery and Mapping Agency)*  
*Photographic Interpretation Center (NPIC), United States National*  
*Photography, High-Altitude*  
*RADAR, Synthetic Aperture*  
*Satellites, Non-Governmental High Resolution*

---

## Marine Mammal Program

---

**■ JULI BERWALD**

The U.S. Navy has used marine mammals, or cetaceans, for military purposes since the late 1950s. Atlantic bottlenose dolphins, Pacific white-sided dolphins, and California sea lions are currently used in military operations, and training has also been conducted with belugas, killer whales, and pilot whales. Because dolphins have superior sonar that is currently unmatched by technology and sea lions have an excellent sense of directional hearing along with sensitive low light vision, these marine mammals are extremely well suited for search and rescue and swimmer defense operations.

**History of marine mammals in the military.** In the 1959, the United States Navy established a marine mammal program at Marineland near Los Angeles, California. Naval researchers were initially interested in studying the hydrodynamics of dolphin swimming in order to better understand boat and submarine design. Dolphins can attain high swimming speeds and can maintain those speeds for long periods of time. Marine scientists found that the dolphin's keen sense of echolocation was ideal for finding lost equipment on the sea floor and for locating enemy mines and torpedoes. In addition, dolphins are extremely intelligent and trainable. One of the first dolphins involved with the program was a Pacific white-sided dolphin named Notty.

In 1962, the marine mammal program was moved to Point Magu, California. Three years later, the Point Magu program established an underwater laboratory called Sea

Lab II, which was 200 feet below the surface of the ocean. There a dolphin named Tuffy was trained to work with divers in experiments designed to see if the use of dolphins might help circumvent the dangers to humans inherent in deepwater diving. Tuffy's work also showed that dolphins could easily be trained to work without tethers in the open ocean. The successes of Sea Lab II led to the establishment of the Advanced Marine Biological Systems (AMBS) program, which currently funds military marine mammal programs.

In 1967, the marine mammal program was moved from Point Magu to Point Loma in San Diego, and a separate marine mammal training facility was opened in the Marine Corps Air Station in Kaneohe Bay, Hawaii. Both of these programs investigated the physiology and behavior of cetaceans, developed techniques for medical diagnosis and treatment, and worked to understand the communicative noises made by dolphins. In Hawaii, research was also conducted on the reproductive physiology of dolphins. In addition, investigators studied the cost and safety benefits of using marine mammals. In 1993, the facility at Kaneohe Bay was closed and most of the marine mammals were relocated to Point Loma.

During the Cold War, the Soviet Union also developed a marine mammal program. Dolphins were trained to search for underwater explosives and were used to guard coastal waters from attack. After the dissolution of the Soviet Union, the dolphins became part of the Ukrainian navy. In 1997, the Ukrainian navy donated the dolphins to a program that uses the animals in therapy for disabled children.

**Training and maintenance.** The U.S. Navy maintains the marine mammals in their training and operational programs in open-mesh enclosures in bays and harbors in the ocean. This allows the dolphins to experience their natural echolocation and social environments. During training, the animals are untethered in the open ocean. All operational training is based on positive reinforcement, using food for rewards. Animals are not punished for failure to perform tasks by withholding food. Survival rates for the marine mammals maintained by the navy are between 95 and 100 percent. During thousands of training exercises in the open ocean over a 30-year period, only seven animals have not returned to their enclosures.

Several groups have criticized the navy's marine mammal program, citing undue stress to and mistreatment of animals used for military purposes. In the 1980s, the Progressive Animal Welfare Society (PAWS) successfully sued the navy to halt its marine mammal program in Washington State. However, a committee appointed by the president reviewed the program in 1988 and 1990 and gave satisfactory or outstanding ratings to all aspects of the program. The National Marine Fisheries (NMFs) reported that survival rates of dolphins in the program were the highest of all organizations maintaining large numbers of cetaceans.



U.S. Navy Sergeant Andrew Garrett with K-Dog, a bottle-nose dolphin who was being trained for mine-clearing operations in support of Operation Iraqi Freedom, 2003. AP/WIDE WORLD PHOTOS.

**Marine Mammal Systems.** The navy currently operates four Marine Mammal Systems (MMS) as part of its fleet. An operational MMS consists of four to eight marine mammals, an officer-in-charge, and several enlisted personnel. Before a MMS is approved for operations, it undergoes the same type of rigorous testing as other operational naval systems. It must prove effective and reliable as well as cost effective. Marine Mammal Systems are highly transportable and can be airlifted to any operational site. SPAWAR (Space and Naval Systems Center, San Diego) supports a deployed MMS, replenishing animals and providing training, documentation, and personnel.

The four operational MMS include both dolphin and sea lion systems. Mk4 and Mk7 are dolphin mine detection and location systems. They can be deployed from a ship in order to search for and mark mines that are tethered to the ocean floor. Mk5 is a sea lion mine detection system, which can detect mines to a depth of 1000 feet. The sea lions are trained to attach a grabber device to a mine so that naval personnel can recover it. Mk6 is a dolphin swimmer defense system. Dolphins are trained to locate an intruder trying to come ashore via the ocean.

Although dolphins and sea lions are the only marine mammals currently used in military operations, pilot whales, killer whales and beluga whales have also been involved with object search and recovery. These cetaceans have the ability to dive to extreme depths, much beyond those attainable by human divers. A project called Deep Ops studied the abilities of pilot whales and killer whales to recover objects from deep depths. The pilot whale was able to successfully recover a dummy torpedo from a depth of 1,654 feet using a gas-inflated recovery device. The killer whales recovered objects from 500 and 850 feet. Belugas were able to dive to 2,100 feet and were able to recover dummy torpedoes from 1,300 feet.

**Marine mammal deployments.** The military first used the dolphin swimmer detection system in the Vietnam War in 1970. This successful operation, which involved dolphins patrolling the waters near warships, brought an end to underwater sabotage in Cam Ranh Bay.

In 1987 and 1988, the navy used dolphins for mine surveillance in waters off Bahrain in the Persian Gulf. The animals patrolled the waters for mines and escorted Kuwaiti tankers through areas where the Iranian military was attempting to disrupt oil shipments.

Marine mammal systems were in operation during the Republican Party Convention in 1996. Both dolphin mine detection and location systems and sea lion swimmer defense systems were used to protect the waters off of San Diego from terrorist attack.

After British forces took control of the southern Iraq port city of Umm Qasr in 2003, the U.S. Navy brought in Atlantic bottlenose dolphins to search the bay for mines and mark them for destruction by human divers. Sea lions

were also deployed around ships in Bahrain to detect and defend against armed swimmers. These sea lions were trained to attach floater devices to intruders so that security officers could apprehend them.

#### ■ FURTHER READING:

##### ELECTRONIC:

Bulletin of Atomic Scientists. "U.S., Ukraine at cross purposes." <<http://www.bullatomsci.org/issues/1997/nd97/nd97bulletins.html>> (April 22, 2003).

Dolphins of War. <<http://www.angelfire.com/nj4/navy/dolphins/>> (April 22, 2003).

MSNBC News. "Dolphins go to front lines in Iraq war." <<http://www.msnbc.com/news/890520.asp>> (March 25, 2003).

Public Broadcasting System. "The Story of Navy Dolphins." <<http://www.pbs.org/wgbh/pages/frontline/shows/whales/etc/navycron.html>> (April 22, 2003).

U.S. Navy Marine Mammal Program. <<http://www.spawar.navy.mil/sandiego/technology/mammals/>> (April 22, 2003).

#### SEE ALSO

*Unexploded Ordnance and Mines*

## McCarthyism

#### ■ JOSEPH PATTERSON HYDER

In the early 1950s, Joseph McCarthy, a U.S. Senator from Wisconsin, conducted highly publicized congressional hearings to uncover subversive elements within American culture, government, and military. For over three years, McCarthy used questionable means to uncover information about suspects. The McCarthy era represents the height of the post-war "Red scare" and demonstrates the degree to which paranoia about subversive communist activities had gripped America.

The wartime Alien Registration Act of 1940 laid the foundation for McCarthyism. This act required that all aliens over the age of 14 residing in the United States register with the American government. Each resident alien had to file a report detailing his or her political beliefs and work status. The act also made it illegal for anyone to plan to overthrow the government of the United States.

The Alien Registration Act had a twofold purpose. First, with American involvement in World War II likely, Congress hoped the act would help identify potential wartime saboteurs. The government wanted to avoid a repeat of the situation in World War I, when German-supported saboteurs and German sympathizers targeted



Dalton Trumbo, left, and John Howard Lawson, two screenwriters of the Hollywood Ten, smile and wave from inside a U.S. Marshal's van after receiving prison sentences for refusing to testify before the House Un-American Activities Committee. AP/WIDE WORLD PHOTOS.

American industry and shipping that aided the European war effort. By acquiring a detailed work history of aliens, the government sought to identify potential problems before they occurred. The second and primary objective of the Alien Registration Act was to identify elements of the American Communist Party or other socialist organizations.

It was subsequently determined that the existing House Un-American Activities Committee (HUAC) would serve as the body that would seek out subversive elements. In 1947, HUAC began a campaign to rid Hollywood of all leftist elements. In a series of highly publicized congressional hearings, some individuals in the entertainment industry identified their peers as belonging to questionable leftist organizations, including the American Communist Party.

In an effort to avoid further embarrassing hearings and to regain public trust, Hollywood studios drew up a blacklist of individuals suspected of belonging to or having an interest in subversive organizations. These individuals found it difficult to work in Hollywood until they

had cleared their names before HUAC. The blacklist included many well-known celebrities, including Charlie Chaplain, Burl Ives, Leonard Bernstein, Aaron Copeland, and Arthur Miller.

The Hollywood blacklist and the HUAC hearings fed the atmosphere of suspicion that gripped American society. To the public, the threat of a complex communist plot to infiltrate American society and government seemed tangible. The high-profile HUAC hearings, combined with the well-publicized Rosenberg and Alger Hiss trials, served to reinforce this sentiment. In the fall of 1949, the government began a crackdown, arresting most of the leadership of the American Communist Party and charging them under the Alien Registration Act.

In February 1950, Joseph McCarthy became involved in the search for subversive elements within the government. McCarthy claimed to have a list containing the names of State Department employees belonging to the American Communist Party. McCarthy's list did not contain any arcane knowledge, having been compiled by the

State Department several years earlier following an internal investigation. Additionally, most of the names were on the list for other questionable behaviors. Few members on the list had any current or previous ties to the Communist Party.

McCarthy took to the pulpit when he became chairman of the Government Committee on Operations of the Senate. Using his position, McCarthy began investigating possible Communist infiltration of various government agencies. McCarthy worked closely with the Federal Bureau of Investigation and his close friend, J. Edgar Hoover. The FBI supplied McCarthy with the information that he needed to keep his committee hearings effective. Government employees found to have ties to the Communist Party or other left-wing groups were removed from office and forced to divulge the names of other individuals affiliated with leftist organizations.

McCarthy's committee also targeted the Overseas Library Program. The Government Committee on Operations of the Senate identified and banned over 30,000 books thought to have been written by communist sympathizers or to contain procommunist themes. Many public libraries across the United States removed these books from their shelves.

McCarthy's operations further expanded into the realm of American politics. His committee conducted disinformation campaigns to thwart the reelection bids of politicians that opposed him. McCarthy even targeted the Truman administration, including President Harry S. Truman himself and cabinet member George Marshall, the renowned architect of the postwar Marshall Plan, for supporting the New Deal and for being perceived as soft on communism in Korea. McCarthy supported Dwight D. Eisenhower's presidential campaign in 1952, and in return, Eisenhower allowed McCarthy to continue his anti-Communist hearings.

In October 1953, after nearly three years of targeting civilian agencies, McCarthy set his sights on identifying and removing subversive elements within the United States Army. Eisenhower, a former army general, decided to stop him. Vice-president Richard M. Nixon spoke out, asserting that McCarthy was motivated not by concern for his country but by a desire for personal aggrandizement. It was revealed that McCarthy had tried to prevent the army from drafting one of his staff members, G. David Schine. After failing in that attempt, McCarthy and his chief counsel, Roy Cohn, had petitioned Stevens to grant special privileges to Schine. The Schine affair prompted McCarthy to target Secretary Stevens: when Stevens refused his request, McCarthy claimed that the army was holding Schine hostage in order to prevent his committee from uncovering communist elements within their ranks.

McCarthy determined that Congress should investigate the matter. He also sealed his fate by allowing television cameras to air the Army-McCarthy hearings. During the hearings, McCarthy and Cohn sought to characterize

the army as an organization riddled with subversive elements. Throughout the hearings, McCarthy appeared rude to an attentive television audience. On the other hand, a personable attorney, Joseph Welch, represented the army. It was Welch who ultimately destroyed McCarthy's credibility with his retort to McCarthy, "Have you no sense of decency, sir, at long last? Have you left no sense of decency?" A bewildered McCarthy did not realize that the power that he once wielded had been crushed before a national television audience. In December 1954, Congress censured Joseph McCarthy by a vote of 67–22.

#### ■ FURTHER READING :

##### BOOKS:

- Fried, Albert. *McCarthyism: The Great American Red Scare: A Documentary History*. Oxford: Oxford University Press, 1996.
- Reeves, Thomas C. *The Life and Times of Joe McCarthy: A Biography*. Madison, WI: Madison Books, 1997.
- Schrecker, Ellen. *The Age of McCarthyism*. New York: St. Martin's, 1994.

##### SEE ALSO

- Cold War (1945–1950), The Start of the Atomic Age*  
*KGB (Komitet Gosudarstvennoi Bezopasnosti, USSR Committee of State Security)*  
*Rosenberg (Ethel and Julius) Espionage Case*  
*Venona*

---

## Measurement and Signatures Intelligence (MASINT)

---

Measurement and signature intelligence (MASINT) is the term for forms of information gathered by analysis of signals (SIGINT), imagery (IMINT), or data acquired through human contact (HUMINT). In the United States, MASINT operations are directed by the Central Measurement and Signatures Office, usually designated as Central MASINT Office or CMO, which is an office of the Defense Intelligence Agency (DIA).

Under the heading of MASINT are the following subcategories: acoustic intelligence (ACINT), infrared intelligence (IRINT), laser intelligence (LASINT), nuclear intelligence (NUCINT), optical intelligence (OPINT), and unintentional radiation intelligence (RINT).

**Components of MASINT.** ACINT, as its name implies, involves the collection and analysis of data derived from sound

waves. Most notable among these are the acoustic markings or “signatures” of military vessels and the weapons they carry, which can be detected by sonar (SOund NAVigation and Ranging) devices underwater. There is some overlap with LASINT, which can be used for audio monitoring. A laser is an extremely narrow, powerful, and focused beam of light. In the LASINT context, a laser beam directed at a closed room can be used to detect the vibrations produced by sound waves.

The term OPINT encompasses all intelligence derived across the spectrum of visible light, as well as light that has been made visible. It is contrasted with IMINT, which is concerned specifically with electronically generated images. Some of the visible material that falls under the purview of OPINT may have been obtained by special equipment that captures light from the infrared portion of the electromagnetic spectrum, and thus once again there may be some overlap, in this case with IRINT.

Infrared waves (lower in frequency than the red, or lowest-frequency, end of the visible spectrum) may also provide a means for radio communication. For instance, in the 1960s, West Germany developed a device that sent and received audible messages, using the infrared range as a medium of transmission. (By contrast, ordinary radio and television transmission occurs at frequencies much lower than that of infrared light.)

Unintentional radiation intelligence (RINT) also involves monitoring of the electromagnetic spectrum, although in this case, for non-information-bearing elements of intelligence. For example, highly radioactive material of the type that might be used in a sophisticated nuclear device, may emit gamma rays, which occupy the highest energy level in the electromagnetic spectrum. Once more, there may be overlap with nuclear intelligence or NUCINT, which is defined as information derived from the collection and analysis of radiation from radioactive sources.

**The U.S. Central MASINT Office.** The office responsible for MASINT is the Defense Intelligence Agency’s CMO. By 1986, the U.S. intelligence community had come to recognize the need for a MASINT office, and in that year formed the Intelligence Community Staff MASINT Committee to oversee all relevant activities. As part of the 1992 reorganization of the intelligence community, the secretary of defense and the director of the CIA gave the director of DIA responsibility over national and defense MASINT. A year later, DIA established CMO, which reports to the director of DIA.

CMO consists of four divisions, designated as CMO–1, 2, 3, and 4. The first of these is responsible for developing national and defense policy, including long-term plans, and for establishing the interface between MASINT and other intelligence-gathering disciplines. CMO-2 is responsible for resource management, or the management of MASINT assets nationally and worldwide. CMO-3 oversees

MASINT collection operations, and is responsible for time-sensitive and short-turnaround jobs. CMO–4, the Advanced Concepts Division, manages research, development, testing, and evaluation.

#### ■ FURTHER READING:

##### BOOKS:

Richelson, Jeffrey T. *The U.S. Intelligence Community*, third edition. Boulder, CO: Westview Press, 1995.

Scanlon, Charles Francis. *In Defense of the Nation: DIA at Forty Years*. Washington, D.C.: Defense Intelligence Agency, 2002.

##### ELECTRONIC:

Evaluation Report on Measurement and Signature Intelligence. <[http://www.fas.org/irp/program/masint\\_evaluation\\_rep.htm](http://www.fas.org/irp/program/masint_evaluation_rep.htm)> (January 17, 2003).

##### SEE ALSO

*Lasers*  
*Nuclear Detection Devices*

---

## Metal Detectors

---

#### ■ LARRY GILMAN

Metal detectors use electromagnetic fields to detect the presence of metallic objects. They exist in a variety of walk-through, hand-held, and vehicle-mounted models and are used to search personnel for hidden metallic objects at entrances to airports, public schools, courthouses, and other guarded spaces; to hunt for landmines, archaeological artifacts, and miscellaneous valuables; and for the detection of hidden or unwanted metallic objects in industry and construction. Metal detectors detect metallic objects, but do not image them. An x-ray baggage scanner, for example, is not classed as a metal detector because it images metallic objects rather than merely detecting their presence.

Metal detectors use electromagnetism in two fundamentally different ways, active and passive. (1) Active detection methods illuminate some detection space—the opening of a walk-through portal, for example, or the space directly in front of a hand-held unit—with a time-varying electromagnetic field. Energy reflected from or passing through the detection space is affected by the presence of conductive material in that space; the detector detects metal by measuring these effects. (2) Passive detection methods do not illuminate the detection space, but take advantage of the fact that every unshielded detection space is already permeated by the Earth’s natural





FBI agents use metal detectors to search for evidence in a series of sniper attacks that occurred in the Washington, D.C., area in 2002. AP/WIDE WORLD PHOTOS.

magnetic field. Ferromagnetic objects moving through the detection space cause temporary, but detectable changes in this natural field. (Ferromagnetic objects are made of metals, such as iron, that are capable of being magnetized; many metals, such as aluminum, are conducting but not ferromagnetic, and cannot be detected by passive means.)

**Walk-through metal detectors.** Walk-through or portal detectors are common in airports, public buildings, and military installations. Their portals are bracketed with two large coils or loop-type antennae, one a source and the other a detector. Electromagnetic waves (in this case, low-frequency radio waves) are emitted by the source coil into the detection space. When the electromagnetic field of the transmitted wave impinges on a conducting object, it induces transient currents on the surface of the object; these currents, in turn, radiate electromagnetic waves. These secondary waves are sensed by the detector coil.

**Hand-carried metal detectors.** Metal detectors small enough to be hand-held are often used at security checkpoints to localize metal objects whose presence has been detected by a walk-through system. Some units are designed to be carried by a pedestrian scanning for metal objects in the ground (e.g., nails, loose change, landmines). All such

devices operate on variations of the same physical principle as the walk-through metal detector, that is, they emit time-varying electromagnetic fields and listen for waves coming back from conducting objects. Some ground-search models further analyze the returned fields to distinguish various common metals from each other. Hand-carried metal detectors have long been used to search for landmines; however, modern land mines are often made largely of plastic to avoid this cheap and obvious countermeasure. New technologies, especially neutron activation analysis and ground-penetrating radar, are being developed to search for nonmetallic landmines.

**Gradiometer metal detectors.** Gradiometer metal detectors are passive systems that exploit the effect of moving ferromagnetic objects on the earth's magnetic field. A gradiometer is an instrument that measures a gradient—the difference in magnitude between two points—in a magnetic field. When a ferromagnetic object moves through a gradiometer metal detector's detection space, it causes a temporary disturbance in the earth's magnetic field, and this disturbance (if large enough) is detected. Gradiometer metal detectors are usually walk-through devices, but can also be mounted on a vehicle such as a police car, with the intent of detecting ferromagnetic weapons (e.g., guns) borne by persons approaching the vehicle. Gradiometer metal detectors are limited to the detection of ferromagnetic objects and so are not suitable for security situations

where a would-be evader of the system is likely to have access to nonferromagnetic weapons.

**Magnetic imaging portals.** The magnetic imaging portal is a relatively new technology. Like traditional walk-through metal detectors, it illuminates its detection space with radio-frequency electromagnetic waves; however, it does so using a number of small antennas arranged ringlike around its portal, pointing inward. Each of these antennas transmits in turn to the antennas on the far side of the array; each antenna acts as a receiver whenever it is not transmitting. A complete scan of the detection space can take place in the time it takes a person to walk through the portal. Using computational techniques adapted from computed axial tomography (CAT) scanning, a crude image of the person (or other object) inside the portal is calculated and displayed. The magnetic imaging portal may for some purposes be classed as a metal detector rather than as an imaging system because it does not produce a detailed image of the metal object detected, but only reveals its location and approximate size.

■ FURTHER READING:

ELECTRONIC:

“Guide to the Technologies of Concealed Weapon and Contraband Imaging and Detection (NIJ Guide 602–00).” Institute of Justice, US Department of Justice. February 2001. <<http://www.ojp.usdoj.gov/nij/pubs-sum/184432.htm>> (April 23, 2003).

## Meteorology and Weather Alteration

■ AGNES GALAMBOSI

Up to 40 percent of the estimated \$10 trillion U.S. economy is affected by weather and climate each year. The National Aeronautics and Space Administration (NASA) and the National Oceanic and Atmospheric Administration (NOAA) are the two U.S. agencies with primary responsibility for developing technology related to earth observation (e.g., the design and operation of weather satellites) and meteorological monitoring.

Meteorology is a science that studies the processes and phenomena of the atmosphere. Meteorology consists of many areas: physical meteorology, dealing with physical aspects of the atmosphere such as rain or cloud formation; synoptic meteorology, the analysis and forecast of large-scale weather systems; dynamic meteorology, which is based on the laws of theoretical physics; climatology,

the study of the climate of an area; aviation meteorology, researching weather information for aviation; atmospheric chemistry, examining the chemical composition and processes in the atmosphere; atmospheric optics, analyzing the optical phenomena of the atmosphere such as halos or rainbows; or agricultural meteorology, studying the relationship between weather and vegetation.

In his book *Meteorologica*, written c. 340 B.C., Greek philosopher and scientist Aristotle (384 – 322 B.C.) was the first to record the use of the term meteorology. Aristotle’s work summarized the knowledge of the day concerning atmospheric phenomena. He speculatively wrote about clouds, rain, snow, wind, and climatic changes, and although many of his findings later proved to be incorrect, many of them were insightful.

The fourteenth-century invention of weather measuring instruments made scientific study of atmospheric phenomena possible, but it was the seventeenth century inventions of the thermometer, barometer (a device used to measure atmospheric pressure), and anemometer (a device used for measuring wind speed) that laid the foundation for modern meteorological observation. In 1802, the first cloud classification system was formulated, and in 1805, a wind scale was first introduced. These measuring instruments and new ideas made possible the gathering of actual data from the atmosphere that, in turn, provided the basis for the advancement of scientific theories involving atmospheric structure, properties (pressure, temperature, humidity, etc.), and governing physical laws.

In the early 1840s, the first weather forecasting services started with ability to transmit observational data via telegraph. At that time, meteorology was still in the descriptive phase, still on an empirical basis with few scientific theories.

Meteorological science was spurred by World War I military demands. Norwegian physicist Vilhelm Bjerknes (1862–1951) introduced a modern meteorological theory stating that weather patterns in the temperate middle latitudes are the results of the interaction between warm and cold air masses. His description of atmospheric phenomena and forecasting techniques were based on the laws of physics and provided a template for modern dynamic meteorological modeling. By assuming a given set of atmospheric conditions to which were applied governing physical laws, meteorologists could make predictions about future weather and climatic conditions.

By the 1940s, upper-level measurements of pressure, temperature, wind, and humidity provided detailed insight into the vertical properties of the atmosphere. In the 1940s, Englishman R. C. Sutcliffe and Swede S. Peterssen developed three-dimensional analysis and forecasting methods. American military pilots flying above the Pacific during World War II discovered a strong stream of air rapidly flowing from west to east, which became known as the jet stream—an important factor in the movement of air masses. Weather radar first came into use in the United



The Norman Doppler Radar stands beneath ominous-looking clouds at the National Severe Storms Laboratory in Norman, Oklahoma. AP/WIDE WORLD PHOTOS.

States in 1949 with the efforts of Horace Byers (1906–1998) and R. R. Braham. Conventional weather radar shows precipitation location and intensity. Ultimately, the development of radar, rockets, and satellites greatly improved data collection and weather forecasting.

In 1946, the process of cloud seeding made possible early weather modification experiments. In the 1950s, radar became important for detecting precipitation of a remote area. Also in the 1950s, with the invention of the computer, weather forecasting became not only quicker but also more reliable, because the computers could more rapidly solve the mathematical equations of atmospheric models. In 1960, the first meteorological satellite was launched.

Satellites now give three-dimensional data to high-speed computers for faster and more precise weather predictions. Modern computers are capable of plotting observational data, and performing both short term and long term modeling analysis ranging from next day weather forecasting to decades long climatic models. Even so, the computers still have their capacity limits, the models still have many uncertainties, and the effects of the atmosphere on our complex society and environment can be serious. Many complicated issues remain at the forefront of meteorology, including air pollution, global warming, El Niño events, climate change, ozone hole or acid rain,

making meteorology a scientific area still fraught with challenges and unanswered questions.

**Weather forecasting.** Weather forecasting is the attempt by meteorologists to predict the state of the atmosphere at a near future time and the weather conditions that may be expected. Many military planners consider weather to be a “force multiplier” (i.e., forces prepared to operate effectively in adverse conditions can fare substantially better than unprepared forces). Accurate weather forecasts are especially critical to the tactical operation of aviation and naval forces.

In the United States, weather forecasting is the responsibility of the National Weather Service (NWS), a division of the National Oceanic and Atmospheric Administration (NOAA) of the Department of Commerce. NWS maintains more than 400 field offices and observatories in all 50 states and overseas. The future modernized structure of the NWS will include 116 weather forecast offices (WFO) and 13 river forecast centers, all collocated with WFOs. WFOs also collect data from ships at sea all over the world and from meteorological satellites. Each year the NWS collects nearly four million pieces of information about atmospheric conditions from these sources.

The information collected by WFOs is used in the weather forecasting work of NWS. The data is processed

by nine National Centers for Environmental Prediction (NCEP). Each center has a specific weather-related responsibility: seven of the centers focus on weather prediction—the Aviation Weather Center, the Climate Prediction Center, the Hydrometeorological Prediction Center, the Marine Prediction Center, the Space Environment Center, the Storm Prediction Center, and the Tropical Prediction Center. The other two centers—the Environmental Prediction Center and NCEP Central Operations—develop and run complex computer models of the atmosphere and provide support to the other centers. Severe weather systems such as thunderstorms, tornadoes, and hurricanes are monitored at the National Storm Prediction Center in Norman, Oklahoma, and the National Hurricane Center in Miami, Florida. Hurricane watches and warnings are issued by the National Hurricane Center's Tropical Prediction Center in Miami serving the Atlantic, Caribbean, Gulf of Mexico, and eastern Pacific Ocean) and by the Forecast Office in Honolulu (serving the central Pacific). WFOs, other government agencies, and private meteorological services rely on NCEP's information, and many of the weather forecasts in the paper and on radio and television originate at NCEP.

Global weather data are collected at more than 1,000 observation points around the world and then sent to central stations maintained by the World Meteorological Organization, a division of the United Nations. Global data also is sent to NWS's NCEPs for analysis and publication.

According to steady-state or trend models, weather conditions are strongly influenced by the movement of air masses that often can be charted quite accurately. A weather map might show that a cold front is moving across the great plains of the United States from west to east with an average speed of 10 mph (16 kph). It might be reasonable to predict that the front would reach a place 100 mi (1,609 km) to the east in a matter of 10 hours. Since characteristic types of weather often are associated with cold fronts it then might be reasonable to predict the weather at locations east of the front with some degree of confidence.

A similar approach to forecasting is called the analogue method because it uses analogies between existing weather maps and similar maps from the past. For example, suppose a weather map for December 10, 2003, is found to be almost identical with a weather map for January 8, 1996. Because the weather for the earlier date is already known it might be reasonable to predict similar weather patterns for the later date.

Another form of weather forecasting makes use of statistical probability. In some locations on Earth's surface, one can safely predict the weather because a consistent pattern has already been established. In parts of Peru, it rains no more than a few inches per century. A weather forecaster in this region might feel confident that he or she could predict clear skies for tomorrow with a 99.9% chance of being correct.

The complexity of atmospheric conditions is reflected in the fact that none of the forecasting methods outlined above is dependable for more than a few days, at best. This reality does not prevent meteorologists from attempting to make long-term forecasts, but accuracy declines as the forecast interval increases.

The basis for long-range forecasting is a statistical analysis of weather conditions over an area in the past. For example, a forecaster might determine that the average snow fall in December in Grand Rapids, Michigan, over the past 30 years had been 15.8 in (40.1 cm). A reasonable way to try estimating next year's snowfall in Grand Rapids would be to assume that it might be close to 15.8 inches (40.1 cm). This kind of statistical data is augmented by studies of global conditions such as winds in the upper atmosphere and ocean temperatures. If a forecaster knows that the jet stream over Canada has been diverted southward from its normal flow for a period of months, that change might alter precipitation patterns over Grand Rapids over the next few months.

The term numerical weather prediction is something of a misnomer because all forms of forecasting make use of numerical data such as temperature, atmospheric pressure, and humidity. More precisely, numerical weather prediction refers to forecasts that are obtained by using complex mathematical calculations carried out with high-speed computers.

Numerical weather prediction is based on mathematical models of the atmosphere. A mathematical model is a system of equations that attempts to describe the properties of the atmosphere and changes that may take place within it. These equations can be written because the gases that comprise the atmosphere obey the same physical and chemical laws that gases on earth's surface follow. For example, Charles' Law says that when a gas is heated it tends to expand. This law applies to gases in the atmosphere as it does to gases in a laboratory.

The technical problem that meteorologists face is that atmospheric gases are influenced by many different physical and chemical factors at the same time. A gas that expands according to Charles' Law may also be decomposing because of chemical forces acting on it. Meteorologists select a group of equations that describe the conditions of the atmosphere as completely as possible for any one location at any one time. This set of equations can never be complete because even a computer is limited as to the number of calculations it can complete in a reasonable time. Thus, meteorologists must select the factors they predict will be the most important in influencing the development of atmospheric conditions.

The accuracy of numerical weather predictions depends primarily on two factors. First, the more data that is available to a computer the more accurate its results. Second, the faster the speed of the computer the more calculations it can perform and the more accurate its report will be. In the period from 1955 (when computers

were first used in weather forecasting) to the current time, the percent skill of forecasts has improved from about 30 percent to more than 60 percent. The percent skill measure was invented to describe the likelihood that a weather forecast will be better than pure chance.

Today, an accurate next-day forecast often is possible. For periods of less than a day, a forecast covering an area of 100 sq mi (259 sq km) is likely to be quite dependable.

In the 1990s, the more advanced Doppler radar, which can continuously measure wind speed in addition to precipitation location and intensity, came into wide use. Using mathematical models to automatically analyze data, calculators and computers gave meteorologists the ability to process large amounts of data and make complex calculations quickly. Today the integration of communications, remote sensing, and computer systems makes it possible to predict the weather almost simultaneously. Weather satellites, the first launched in 1960, can now produce sequence photography showing cloud and frontal movements, water-vapor concentrations, and temperature changes.

In addition to directly impacting operational effectiveness of military and other security forces. Emergency planners rely on accurate forecast maps to predict the dissemination patterns of nuclear, chemical, and biological materials.

**Cloud seeding.** Starting in the 1940s, researchers experimented with modifying precipitation patterns.

After about three years of investigative work at the General Electric Research Laboratory in Schenectady, New York, researchers Irving Langmuir and his assistant, Vincent Joseph Schaefer, created the first human-made rainfall. Their work had originated as war-influenced research on airplane wing icing. On November 13, 1946, Schaefer sprinkled several pounds of dry ice (frozen carbon dioxide) from an airplane into a supercooled cloud, a cloud in which the water droplets remain liquid in sub-zero temperatures. He then flew under the cloud to experience a self-induced snowfall. The snow changed to rain by the time it reached Langmuir, who was observing the experiment on the ground.

Langmuir and Schaefer selected dry ice as cloud “seed” for its quick cooling ability. As the dry ice travels through the cloud, the water vapor behind it condenses into rain-producing crystals. As the crystals gain weight, they begin to fall and grow larger as they collide with other droplets.

Another General Electric scientist who had worked with Langmuir and Schaefer, Bernard Vonnegut, developed a different cloud-seeding strategy. The formation of water droplets requires microscopic nuclei. Under natural conditions, these nuclei can consist of dust, smoke, or sea salt particles. Instead of using dry ice as a catalyst, Vonnegut decided to use substitute nuclei around which the water droplets in the cloud could condense. He chose silver iodide as this substitute because the shape of its crystals

resembled the shape of the ice crystals he was attempting to create.

The silver iodide was not only successful, it had practical advantages over dry ice. It could be distributed from the ground through the use of cannons, smoke generators, and natural cumulonimbus cloud updrafts. Also, it could be stored indefinitely at room temperature.

A nucleation event is the process of condensation or aggregation (gathering) that results in the formation of larger drops or crystals around a material that acts as a structural nucleus around which such condensation or aggregation proceeds. Moreover, the introduction of such structural nuclei can often induce the processes of condensation or crystal growth. Accordingly, nucleation is one of the ways that a phase transition can take place in a material.

In addition to their importance in explaining a wide variety of geophysical and geochemical phenomena—including crystal formation—the principles of nucleation were used in cloud seeding weather modification experiments where nuclei of inert materials were dispersed into clouds with the hopes of inducing condensation and rainfall.

During a phase transition, a material changes from one form to another. For example, ice melts to form liquid water, or a liquid boils to form a gas. Phase transitions occur due to changes in temperature. Certain transitions occur smoothly throughout the whole material, while others happen suddenly at different points in the material. When the transitions occur suddenly, a bubble forms at the point where the transition began, with the new phase inside the bubble and the old phase outside. The bubble expands, converting more and more of the material into the new phase. The creation of a bubble is called a nucleation event.

Phase transitions are grouped into two categories, known as first order transitions and second order transitions. Nucleation events happen in first order transitions. In this kind of transition, there is an obstacle to the transition occurring smoothly. A prime example is condensation of water vapor to form liquid water. Condensation requires that many water molecules collide and stick together almost simultaneously. This requirement for simultaneous collisions presents a temporary but measurable barrier to the formation of a bubble of liquid phase. Following formation, the bubble expands as more water molecules strike the surface of the bubble and are absorbed into the liquid phase. Because of the obstacle to the phase transition, a liquid may exist in its gaseous state even though the temperature is well below the boiling point.

A liquid in this state is said to be supercooled. Accordingly, in order for a liquid to be supercooled, it must be pure, because dust or other impurities act as nucleation centers. If the liquid is very pure, however, it may remain supercooled for a long time. A supercooled state is termed metastable due to its relatively long lifetime.

The other type of phase transition is called second order, and it proceeds simultaneously throughout the

whole material. An example of a second order transition is the melting of a solid. As the temperature rises, the magnitude of the thermal vibrations of molecules causes the solid to break apart into a liquid form. As long as the solid is in thermal equilibrium and the melting occurs slowly, the transition takes place at the same time everywhere in the solid, rather than taking place through nucleation events at isolated points.

There is general disagreement over the success and practicality of cloud seeding. Opponents of cloud seeding contend that there is no real proof that the precipitation experienced by the seeders is actually of their own making. Proponents, on the other hand, declare that the effect of seeding may be more than local.

Regardless, until the 1990s, when efforts were generally abandoned for lack of scientific proof of their effectiveness, cloud seeding was an accepted part of the strategy to combat drought. During the Vietnam War, the U.S. attempted to deny use of roads and trails to the North Vietnamese by seeding clouds and inducing localized rainfall. The effectiveness of those attempts remains questionable.

#### ■ FURTHER READING:

##### BOOKS:

Hamblin, W. K., and E. H. Christiansen. *Earth's Dynamic Systems*, 9th ed. Upper Saddle River, NJ: Prentice Hall, 2001.

Hancock, P. L., and B. J. Skinner, eds. *The Oxford Companion to the Earth*. New York: Oxford University Press, 2000.

Lutgens, Frederick, K., et al. *The Atmosphere: A Introduction to Meteorology*, 8th ed. Upper Saddle River, NJ: Prentice Hall, 2001.

##### ELECTRONIC:

National Weather Service. "Internet Weather Source." <<http://weather.noaa.gov/>> (March 29, 2003).

National Oceanic and Atmospheric Administration. <<http://www.noaa.gov/>> (March 29, 2003).

##### SEE ALSO

FEMA (United States Federal Emergency Management Agency)

NOAA (National Oceanic & Atmospheric Administration)

## Mexico, Intelligence and Security

The seat of complex ancient civilizations, espionage and intelligence work has long been practiced in Mexico. Mayan societies and great city-states employed spies to seek information about political rivals and assess the strength

of opposing armies. During the age of Spanish colonialism, Indian and Spanish leaders both employed intelligence personnel and diplomats to smuggle weapons, secure peace treaties, act as interpreters, and conduct espionage. After gaining independence from Spanish rule in 1910, Mexico established its own modern intelligence community. However, the nation weathered periodic political and economic turmoil.

Mexico maintains both civilian and military intelligence services, as well as a national police force. The Mexican intelligence community is organized according to the traditional distinctions between domestic and foreign intelligence, though many agencies utilize a multiplicity of intelligence gathering technologies and operational strategies.

The main civilian intelligence organization in Mexico is the *Centro de Información de Seguridad Nacional* (CISEN), or Center for Research on National Security. A government restructuring of the intelligence community established CISEN in 1989. The agency focuses on domestic intelligence and the assessment of threats to national security. The dramatic rise in illegal immigration, organized crime, and illicit drug trafficking have influenced intelligence policy, with increasing CISEN and law enforcement resources being devoted to combat these problems in recent years. CISEN employs human intelligence, as well as technological surveillance, and advises the government on security systems to guard sensitive communications and computer systems.

The *Secretaría de la Defensa Nacional* (SEDENA), Secretariat of National Defense, administers Mexican military intelligence. Though each branch of the Mexican military employs embedded intelligence units, the main military intelligence agency is the S-2 Second Section. S-2 coordinates joint intelligence efforts and processes information gathered by military intelligence operations. Military intelligence focuses on the collection and analysis of foreign intelligence, especially that which pertains to the strength and deployment operations of foreign militaries. Both CISEN and S-2 conduct regular counter-intelligence operations, and both have contributed to international anti-trafficking and anti-terrorism efforts.

#### ■ FURTHER READING:

##### ELECTRONIC:

Central Intelligence Agency. *The World Factbook*, 2002. "Mexico." <<http://www.cia.gov/cia/publications/factbook/geos/mx.html>> (March 30, 2003).

## MI5 (British Security Service)

■ K. LEE LERNER/JUDSON KNIGHT

Best known by its designation MI5, the Security Service is the leading counter-espionage agency working in the

United Kingdom. Its functions are somewhat akin to those of the United States Federal Bureau of Investigation, but MI5 places a much greater emphasis on intelligence, and its operatives have no arrest powers. Formed in 1916, MI5 devoted itself to intelligence operations against the Germans in both world wars, and against Communists in the interwar and postwar periods. During the early Cold War, MI5 suffered a number of embarrassments involving Soviet moles in its midst. From the 1970s onward, it devoted increasing attention to terrorist activities, and in the 1990s, attempted to balance its sensitive security functions with an increased concern for openness with the British public.

**Wartime successes (1909–45).** MI5 grew out of the Secret Service Bureau, created in 1909 to protect the British realm against German infiltrators. At the beginning of World War I, the Home Section of the bureau came under the control of the War Office, which designated it MI5 (the “MI” refers to military intelligence) in 1916. Over the course of the war, MI5 assisted in the arrest of several dozen German operatives in Britain.

Under the direction of Captain Vernon Kell, who served as director-general until 1940, MI5 in the immediate postwar years directed its efforts toward spies associated with the new Communist regime in Russia. It uncovered a major Soviet front operation in 1927, but by the 1930s had begun to focus once again on German infiltration. MI5, led by Sir David Petrie in the war years, apprehended numerous German spies, who were subsequently executed. Also important, it succeeded in turning a number of other Axis operatives, such that the Nazis remained convinced they had an extensive spy network in Britain—although in fact the spies were working against them.

**Soviet infiltration (1946–79).** The postwar years saw some successes, including Operation Engulf, a program of communications interception directed against the Soviets, French, and Egyptians during the Suez Crisis in 1956. MI5 also captured several Soviet operatives, but its achievements were overshadowed by the uncovering of the Cambridge spy ring, whose members served as Soviet moles while working for the British government. Although neither Donald Maclean nor Kim Philby actually worked for MI5, both were under investigation by the agency when they escaped to the other side of the iron curtain in 1949 and 1963, respectively.

Worse revelations were to come. In 1963 it was discovered that Anthony Blunt, who had worked for MI5 in the war years, was also a Soviet agent. Eventually it became apparent that the Soviets had been infiltrating MI5 for most of the postwar period. The list of suspected Soviet agents included some extremely high officials: director-general Sir Roger Hollis (1956–65) and future director-general Sir Michael Hanley (1972–79). These revelations did little to inspire the trust of American intelligence agencies, which cooperated little with MI5 until after the end of Hanley’s tenure.

**Focus on terrorism (1979–present).** By the 1960s, MI5 had become increasingly concerned with terrorism, both by Palestinian and Northern Irish groups. Revelations of Soviet infiltration continued even into the 1980s, when former MI5 operative Michael Bettaney was convicted of espionage on behalf of the KGB. The spy scandals eventually ended, although not so much because of measures MI5 took to counter infiltration, but because of the Soviet Union’s collapse.

During the mid-1980s, MI5 came under intense government scrutiny in the form of an investigation by Britain’s Security Commission. The result of this was the appointment of Sir Anthony Duff to the director-general’s position, and in 1988 Duff took measures to reform the agency. The Security Service Act of 1989 for the first time conferred legal status on MI5, which in December 1991 signaled a new era of openness by announcing the appointment of Stella Rimington as director-general. Rimington became not only its first female director, but the first MI5 chief named in the media.

In 1993, MI5 further demonstrated its openness by publishing a booklet titled *The Security Service*, which described MI5’s six branches of operation: counter-terrorism, counterespionage, counter-subversion, protective security, security intelligence, and record keeping. Meanwhile, in 1992, MI5 was given chief responsibility for British intelligence efforts against Irish terrorism, and over the next seven years it helped bring about 21 convictions for crimes related to terrorism. An emphasis on counterterrorism continued under the leadership of Stephen Lander, appointed director-general in 1996.

## ■ FURTHER READING:

### BOOKS:

- Andrew, Christopher M. *Her Majesty’s Secret Service: The Making of the British Intelligence Community*. New York: Viking, 1986.
- Bar-Joseph, Uri. *Intelligence Intervention in the Politics of Democratic States: The United States, Israel, and Britain*. University Park: Pennsylvania State University Press, 1995.
- The Security Service: MI5*. London: HMSO, 1993.
- West, Nigel. *Molehunt: Searching for Soviet Spies in MI5*. New York: W. Morrow, 1989.

### ELECTRONIC:

- MI5: The Security Service. <<http://www.mi5.gov.uk/>> (April 11, 2003).
- United Kingdom Intelligence Agencies. Federation of American Scientists. <<http://www.fas.org/irp/world/uk/index.html>> (April 11, 2003).

### SEE ALSO

*Cambridge University Spy Ring*  
*Engulf, Operation*

*Moles*  
*United Kingdom, Intelligence and Security*

## MI6 (British Secret Intelligence Service)

■ K. LEE LERNER/JUDSON KNIGHT

Officially known as the Secret Intelligence Service (SIS), MI6 is the chief British foreign intelligence organization, analogous to the United States Central Intelligence Agency. The organization is even more secretive than either its American counterpart, or another well-known member of the British intelligence community, the Security Service, or MI5. Although their functions are quite separate, the MI6 and MI5 share origins, and much of their history in the world wars and Cold War era ran along parallel lines. Yet, whereas MI5 has established a tone of openness with the British public since the early 1990s, MI6 remains guarded concerning the details of its activities.

**World War I and the interwar era.** In 1909, a parliamentary study found evidence of widespread German infiltration, and noted that there was “no organization...for accurately identifying its extent and objectives.” As a result, the British government established the Secret Service Bureau. The bureau was divided into a Home Section under Captain Mansfield Cumming, and a Foreign Section directed by Captain Vernon Kell. The two came to be known, respectively, as “C” and “K.” After World War I broke out, the Foreign Section became MI1(c), and in 1921 the Secret Intelligence Service (SIS), or MI6. Directors of SIS have thenceforth been known by the designation “C” after Cumming, who remained the head of SIS/MI6 until 1923. (The “K” designation, on the other hand, seems to have ended with Kell, first director-general of MI5.)

During World War I, MI6 conducted intelligence operations involving both Germany and Russia, and its operatives and agents included both the author W. Somerset Maugham and the legendary spy Sidney Reilly. In 1919, MI6 took charge of the Government Code & Cypher School (GC&CS), formed from the remains of the British Admiralty’s Room 40, along with a smaller War Office program. GC&CS soon proved successful at breaking ciphers used by the new Bolshevik government. MI6 efforts against both Russia and Germany in the 1930s uncovered evidence of Nazi-Soviet cooperation in the development of weapons technology, but during this era, MI6 also suffered a number of failures, leaving the British government unprepared for such moves as Hitler’s reoccupation of the Rhineland in 1935.

**World War II and the early Cold War.** A new era began for MI6 in November 1939 when, just three months after the outbreak of war, Colonel Stewart Menzies became the new “C.” In that same month, MI6 suffered a major setback when the Germans captured two of its officers in Holland, and obtained considerable information from them under interrogation. Yet, MI6 excelled in its cryptanalytic efforts against the Germans through GC&CS, which in 1942 became the Government Communications Headquarters (GCHQ). Operating from Bletchley Park outside London, GCHQ successfully broke German ciphers on the Enigma machine—the single greatest cryptanalytic success of the war.

Despite the spirit of wartime cooperation with Josef Stalin’s Russia, Menzies in 1944 wisely established a section devoted to Soviet espionage and subversion. Less felicitous was his choice of a section head, Harold (Kim) Philby. In what proved to be a classic case of the fox guarding the chicken coop, Philby would later be exposed as a Soviet spy, and he was not alone; among the many Soviet moles exposed in the two decades after the war were John Cairncross and Charles H. Ellis, both with MI6. Further misfortunes followed as MI6 attempted unsuccessfully to gain intelligence on a Soviet ship docked at Portsmouth, an effort that cost the life of a former navy diver named Lionel Crabb. Yet, MI6 was not without successes in the immediate postwar years; it cultivated a relationship with Soviet intelligence officer Oleg Penkovsky, who would prove a valuable asset to both British and U.S. intelligence.

**From the late Cold War to the present.** By the 1970s, MI6 had turned its attention toward a number of areas other than the Soviet bloc. These included economic espionage, as well as efforts against terrorist groups in Northern Ireland. In the latter capacity, the agency found itself in a turf war with MI5, which was already working on the problems in Northern Ireland. MI6 proved an invaluable asset in the conflict, establishing key links with top Irish Republican Army (IRA) and Sinn Fein figures. Unfortunately, MI6 suffered another embarrassment when two brothers claiming to be MI6 operatives conducted a number of bank robberies in Northern Ireland and claimed that they had been directed to assassinate IRA leaders.

During the 1980s and 1990s, MI6 recovered its standing through successful operations in the Falklands War, Persian Gulf War, and Balkan wars. It gained new statutory grounding with the 1994 passage of the Intelligence Services Act, which defined its responsibilities and functions, as well as those of its chief. The act also set in place a framework of government oversight for MI6 activities. In 1993, Sir Colin McColl became the first MI6 director to be publicly identified. He was replaced in 1994 by Sir David Spedding, and in 1999, Spedding was replaced by Sir Richard B. Dearlove.





The headquarters of the British intelligence services MI6 in London, seen from across the River Thames on the night of September 20, 2000, after an anti-tank rocket was fired at the building. No injuries resulted from the attack, thought to have been perpetrated by the Real IRA. AP/WIDE WORLD PHOTOS.

#### ■ FURTHER READING :

##### BOOKS:

Andrew, Christopher M. *Her Majesty's Secret Service: The Making of the British Intelligence Community*. New York: Viking, 1986.

Dorril, Stephen. *MI6: Inside the Cover World of Her Majesty's Secret Intelligence Service*. New York: Free Press, 2000.

##### ELECTRONIC:

United Kingdom Intelligence Agencies. Federation of American Scientists. <<http://www.fas.org/irp/world/uk/index.html>> (April 11, 2003).

##### SEE ALSO

*Bletchley Park*  
*Cambridge University Spy Ring*  
*Enigma*  
*Room 40*  
*Ultra, Operation*  
*United Kingdom, Intelligence and Security*

## Microbiology: Applications to Espionage, Intelligence, and Security

■ BRIAN HOYLE

Microbiology is concerned with the study of microorganisms such as bacteria, viruses, fungi, protozoa, and algae. There are many facets to the science, ranging from basic studies of organism structure and genetic arrangement, to the development of methods or treatments against those microorganisms that cause diseases in humans, animals, and other living things. A classic example of a strategy against a pathogen (disease-causing organism) is the development of a vaccine. The stimulation of the immune system by the exposure to a component of the particular bacterial or viral strain, or to a weakened, but living version of the virus can confer protection against subsequent exposure to the disease causing bacterium or virus. Microorganisms can also be used for offensive purposes (i.e., biological weapons). The use of recombinant DNA technology—where a gene that specifies the protein of interest

can be removed from the genetic material of one organism and added to the genetic material of the target organism—has enabled the design of biological weapons of frightening potency. For example, the former Soviet Union investigated the insertion of the gene for cobra venom into the genetic material of the influenza virus. The combination of the poison and an easily transmitted virus could have caused swift, catastrophic effects upon its intended population. The science of microbiology contributes in fundamentally important ways to national security, and even influences the gathering of intelligence and espionage activities.

## Microorganisms and Security

The most urgent threat posed by microorganisms to national security is the development of an epidemic. An epidemic is an infection that, because of its ease of transmission from person to person (directly or via an intermediate) affects a large number of people within a very short period of time. The human toll and strain on the health care infrastructure due to naturally occurring epidemics such as influenzae are well known. In the past few decades, the emergence of diseases such as Acquired Immunodeficiency Syndrome (AIDS) and the re-emergence of tuberculosis has further strained the economies of even nations as wealthy as the United States.

The specter of the deliberate use of microorganisms as a weapon—biological warfare—while historically ancient, has taken on new importance in recent years. In the United States, the terrorists attacks of September 11, 2001, were followed by a spate of incidents involving the deliberate release of spores of *Bacillus anthracis*, the bacterium that causes anthrax. While the consequences of these biological attacks were minimized due to a rapid response to track and contain the source, five people died from anthrax, and the incident illustrated the vulnerability of a population to infection.

Even more ominously, evidence indicates that the terrorists responsible for the September 11, 2001, attacks made serious enquiries about the piloting and rental of crop dusting planes. Scenarios envisioning the aerial dispersal of anthrax spores over a major urban center via such a plane indicate that even 100 kilograms of spores carry the potential to kill hundreds of thousands or even millions of people within a few days.

The security threat posed by biological warfare is also ancient. Centuries ago, the decaying bodies of cattle that had died of infections were dumped into wells to poison the drinking water. Even deceased people provided the seed for the spread of infection to an enemy encampment, when the bodies of human victims of anthrax were catapulted over the walls of fortified communities. This military use of microorganisms became frighteningly refined in the twentieth century. Both sides of the conflicts of World Wars I and II researched the development of weapons that would deliver anthrax spores. During World War

II Britain produced millions of anthrax “cakes” that were to be parachuted into Germany. The intent was to decimate the population as well as the food chain.

Other microorganisms, equally as ancient as anthrax, continue to be security threats because of their natural potential to cause massive disease outbreaks, and because of their potential as biological weapons. One example is the disease known as plague, caused by the bacterium *Yersinia pestis*. Another example is smallpox, a disease that is caused by a virus.

The tremendous infectivity of anthrax, plague, and smallpox have caused millions of deaths throughout history. This destructive potential did not escape the attention of governments, such as that of the former Soviet Union, which were interested in developing weapons. Indeed, the microorganisms that cause anthrax, plague, and smallpox have been included in the list of weapons that are strategic weapons. Strategic weapons are those weapons that are capable of destroying entire populations. This puts these microorganisms on the same lethal level as nuclear weapons.

The security threat posed by microorganisms took on an added urgency in the last two decades of the twentieth century, when their potential as a terrorist weapon was recognized. In contrast to bombs and other such munitions, the manufacture of lethal payloads of microorganisms does not require huge manufacturing facilities or large numbers of people. Moreover, the scientific and manufacturing expertise for the development of biological weapons is not beyond the typical microbiologist.

Likewise, the transport of infectious microorganisms can be disguised. Microorganisms can be transported anywhere people can travel. A quantity of anthrax spores that would circulate through the ventilation system of an office building can be contained in a vial carried in someone’s pocket. The ease by which microorganisms can be transported and released (i.e., by a small aircraft) is redefining the nature of security. Methods that are successful in detecting missile silos and troop movements are useless against the deliberate use of microorganisms by a few individuals.

The refinement of genetic engineering technologies has made possible the tailoring of bacteria and viruses to make them more lethal. Microorganisms can normally be rapidly detected using antibodies that recognize a surface antigen. Redesigning a pathogen via genetic engineering so that the surface antigen is different and therefore no longer recognizable to the antibody thwarts the test.

**Natural infections.** A variety of contemporary examples have shown how vulnerable even developed countries are to the spread of infections. From only a few cases in New York City in 1999, the virus that causes West Nile fever has spread through the U.S. and Canada. Thousands of people have contracted West Nile, and the infection shows no signs of abating. Other examples of naturally-occurring infections are legionellosis in Australia, yellow fever and

Creutzfeldt-Jacob disease in Europe, and hantavirus pulmonary syndrome and cryptococcosis in North America.

Modern technology has unexpectedly aided the spread of disease. The classic example is the development of resistance by bacteria to antibiotics. Antibiotics were considered to be “wonder drugs” as recently as the 1960s. However, they have proved to only provide selective pressure for the development of bacteria that are even harder and more capable of causing disease.

A report issued in 2000 by the U.S. National Security Council warned of the security threat posed to the U.S. in the twenty-first century by epidemics of natural infections in underdeveloped, politically volatile countries. The decimation of the next generation of these countries could exacerbate feelings of hostility towards the wealthy nations of the West, putting the U.S. and other developed nations at risk. In 2003, U.S. President George W. Bush pledged 15 billion dollars worth of American aid for the delivery of antiretroviral drugs to African citizens in the effort to halt the spread of AIDS, a naturally occurring infection that affects up to one half of some African populations.

## Microbiological Techniques Relevant to National Security and Intelligence

Various microbiological techniques have long assumed a security role, principally in the detection of infectious microorganisms or toxic components. The ability to rapidly and accurately sequence genetic material came about in the 1990s, largely because of the demands of the Human Genome Project. So did the development (which continues) of software capable of processing the vast amount of genetic data into information that can be used to derive the composition and three-dimensional structure of proteins (i.e., the disciplines of bioinformatics and proteomics). The modeling of protein structures, for example, is important in the development of vaccines that act by blocking the action of some vital bacterial or viral protein.

The lessons learned from the Human Genome Project have been applied to security issues. For example, genetic material can be rapidly isolated from complex samples such as soil and even air (after the air has been filtered to trap the microorganisms on a solid support), and the identity of the microorganism can be determined by the sequencing of the material. The identification is so sensitive that one type (or strain) of bacterium can be distinguished from another. Such analyses were used to show that the strain of *Bacillus anthracis* used in some of the anthrax terrorist attacks of 2001 in the U.S. originated from the government’s Army Medical Institute of Infectious Disease (USAMRIID).

Other technologies permit the rapid detection of bacteria or viruses. For example, the binding of an antibody to

the specific antigen it recognizes can trigger a color development reaction, which is used in test kits to test for the presence of a particular microorganism. Also, genetic amplification techniques like the polymerase chain reaction, or the detection of microorganisms based on target genetic sequences (i.e., amplified fragment length polymorphism analysis, single nucleotide polymorphism analysis) can detect the presence of target sequences of genetic material in samples. The Joint Genome Institute at the Lawrence Berkeley National Laboratory, for example, has catalogued characteristic genetic sequences from a variety of bacterial pathogens.

Other U.S. government laboratories are also developing techniques aimed at thwarting the use of biological weapons. For example, the Los Alamos National Laboratory has developed the Biological Aerosol Sentry and Information System (BASIS), which is intended to provide an early warning of biological incidents. BASIS consists of a series of sampling sites clustered around another site that has been identified as a potential target of sabotage or terrorist/military action. Regular sampling from the sites and analysis of the samples will reveal the presence of a microorganism. The intent is not to prevent the deliberate release of microbes. Rather, the prompt detection of an incident, and subsequent response and mobilization of medical resources is intended to help alleviate the spread of an infection.

**Microorganisms and intelligence.** The national security concerns of microbiology influence intelligence gathering. This influence is two-pronged. First, the need to understand the nature of microbial behavior for the development of defensive strategies such as vaccines requires an open exchange of information and unrestricted research opportunities. However, the sensitive nature of some information, particularly if used by an enemy, can limit the exchange.

The heightened security climate in the U.S. since the terrorist attacks of 2001 has produced a call for limits to information exchange. In March 2002, the chief of staff warned against the open exchange of information concerning scientific advancements that could be utilized in the development of weapons of mass destruction. This issue is contentious, as it goes to the heart of the openness of inquiry that is the hallmark of research science.

Microbiology can also contribute to intelligence by being a direct source of information. It has been successfully demonstrated that messages can be programmed into deoxyribonucleic acid (DNA)—the genetic material that provides the information blueprint for many living organisms—through the arrangement of the components of the DNA. By assigning letters or grammatical symbols to triplets of the components, a section of DNA can be artificially constructed that contains a sequence that, when decoded, yields a message. The artificial sequence can be “spliced” into the DNA sequence of an organism, or even simply blotted onto a pre-determined region of a letter.

The recipient who knew the location of the DNA, could retrieve it and decipher the message.

**Microorganisms and espionage.** The ability to covertly transmit information via genetic sequences also has implications for espionage. Unless someone has knowledge of the means being used to transmit the information, and the technical means to acquire the genetic material and decipher the message, the message will remain secret. Microorganisms also have more traditional uses in espionage; for example, food and water can be deliberately contaminated to make someone ill, so as to compromise a project or a mission.

#### ■ FURTHER READING:

##### BOOKS:

Preston, Richard. *The Demon in the Freezer: A True Story*. New York: Random House, 2002.

##### PERIODICALS:

Atlas, R. N. "National Security and the Biological Research Community." *Science*. no. 298 (2002): 753–754.

Walter, K. "A Two-Pronged Attack on Bioterrorism." *Science & Technology*. (June 2002): 4–11.

##### ELECTRONIC:

Central Intelligence Agency. "The Global Infectious Disease Threat and Its Implications for the United States." January 2000. <<http://www.cia.gov/cia/publications/nie/report/nie99-17d.html>> (November 22, 2002).

##### SEE ALSO

*Anthrax Weaponization*  
*Biological and Biomimetic Systems*  
*Biological and Toxin Weapons Convention*  
*Biological Warfare*  
*Biological Warfare, Advanced Diagnostics*  
*Biological Weapons, Genetic Identification*  
*Bioterrorism*  
*Bioterrorism, Protective Measures*  
*CDC (United States Centers for Disease Control and Prevention)*  
*Infectious Disease, Threats to Security*  
*Pathogens*

## Microchip

#### ■ LARRY GILMAN

Microchips, also termed "integrated circuits" or "chips," are small, thin rectangles of a crystalline semiconductor, usually silicon, that have been inlaid and overlaid with microscopically patterned substances so as to produce

transistors and other electronic components on its surface. It is the components on the chip, not the chip itself, that are micro or too small see with the naked eye. The microchip has made it possible to miniaturize digital computers, communications circuits, controllers, and many other devices. Since 1971, whole computer CPUs (central processing units) have been placed on some microchips; these devices are termed microprocessors.

Manufacture of a microchip begins with the growing of a pure, single crystal of silicon or other semiconducting element. A semiconductor is a substance whose resistance to electrical current is between that of a conductive metal and that of an insulating material such as glass (silicon dioxide, SiO<sub>2</sub>). This large, single crystal is then sawed into thin, disc-shaped wafers 4–12 inches (10–30 cm) across and only .01–.024 inches (.025–.06 cm) thick. One side of each wafer is polished to high precision, then processed to produce on it a number of identical microchips. These are cut apart later, placed in tiny protective boxes or packages, and connected electrically to the outside world by metal pins protruding from the packages.

Producing a microchip requires industrial facilities that cost billions of dollars and must be retooled every few years as technology advances. The basics of the microchip fabrication process, however, remain the same: by bombarding the surface of the wafer with atoms of various elements, impurities or "dopants" can be introduced into its crystalline structure. These atoms have different electron-binding properties from the silicon atoms around them and so populate the crystal either with extra electrons or with holes, gaps that behave much like positively charged electrons. Holes and extra electrons confer specific electrical properties on the regions of the crystal where they reside. By arranging the doped regions containing holes or extra electrons and covering them with multiple, interleaved layers of SiO<sub>2</sub>, polycrystalline silicon (silicon comprised of small, jumbled crystals), and metal strips to conduct current from one place to another, each microchip can be endowed with thousands or millions of microscopic devices. Such chips are termed integrated because the electronic components in them are integral parts of a single, solid object; this both decreases their size and increases their reliability.

The microchip was conceived simultaneously in 1958 by U.S. engineers Jack Kilby and Robert Noyce (1927–1990). In 1962, microchips were used in the guidance computer of the U.S. Minuteman missile (a nuclear-tipped intercontinental ballistic missile based in holes or silos in the American Midwest); the U.S. government also funded early microchip mass-production facilities as part of its Apollo program, for which it requires lightweight digital computers. The Apollo command and lunar modules each had microchip-based computers with 32-kilobyte memories.

For some 40 years, the number of electronic components on an individual microchip has doubled every few years; this trend has been described as Moore's Law ever since 1965, when U.S. engineer Gordon Moore described

the beginning of the trend. Engineers continually strive to fit more electronic components on each microchip; however, this is becoming steadily more difficult as device dimensions decrease toward the atomic scale, where quantum uncertainty renders traditional electronics unreliable. Microchip engineers predict that by about 2020, the exponential increases of the last few decades will cease.

Since their advent, microchips have transformed much of human society. They permit the manufacture of small electronic devices containing many millions of components; they are essential to computers, missiles, "smart" bombs, satellites, communications devices, televisions, aircraft, spacecraft, and motor vehicles. Without microchips the personal computer, cell phone, calculator, Global Positioning System, and many other familiar technologies, both military and civil, would be impossible. As chip complexity increases and cost decreases thanks to improvements in manufacturing technique, new applications are continually being found.

#### ■ FURTHER READING :

##### ELECTRONIC:

Moore, Gordon. "No Exponential is Forever...but We Can Delay 'Forever'." International Solid State Circuits Conference, February 10, 2003. <[ftp://download.intel.com/research/silicon/Gordon\\_Moore\\_ISSCC\\_021003.pdf](ftp://download.intel.com/research/silicon/Gordon_Moore_ISSCC_021003.pdf)> (April 3, 2003).

##### SEE ALSO

*Nanotechnology*

---

## Microfilms

---

#### ■ AGNIESZKA LICHANSKA

Microfilms are miniature films used for photographing objects and documents. The images on these films cannot be seen without an optical aid, either in the form of a magnifying glass or a projector. The main advantages of microfilm include relatively low cost, good image quality, long life and lack of necessity for expensive viewing hardware. Although the images are not visible with a naked eye, only a magnifying glass is needed for reading the microfilms.

**Technology behind microfilms.** The first mini-photographs (8x11mm) were taken using a portable Daguerrean camera produced in 1839. Much later, during the Cold War, the mini-photographs were developed into microdots, tiny photographs of 1mm or less in diameter, looking like a period in a typewritten letter.

The microfilm itself was invented in 1839 by John Dancer. He replaced a slide on the microscope stage with a photographic film and reversed the normal process of microscopy. As a result, instead of seeing a large version of a biological specimen, he was able to produce a miniature image of a large object.

Early microfilms were based on cellulose acetate and over the decades they broke down into acetic acid (vinegar syndrome) and records were destroyed. Currently, there are three types of microfilm: silver halide, diazo, and vesicular. Silver halide films are similar to the traditional film. They consist of the polyester base and silver nitrate emulsion, and are used in cameras for producing the original microfilms. Silver halide films produce the highest resolution and are available as positive and negative image films. If properly stored, their life is estimated to be at least 500 years. Diazo and vesicular films are less stable. Images on diazo films are formed from diazonium salts exposed to ultraviolet light in the presence of ammonium; these images fade with time. The vesicular films produce images by little bubbles inside the film that are sensitive to pressure and can also be destroyed by heat.

Not only did the films (down to 8mm wide) and images become smaller, but cameras were reduced in size and often disguised as everyday items such as watches, cigarette packs, books, and matchboxes. In fact, Kodak produced a camera known as Camera X or Matchbox camera. This camera was used during the Second World War by allied resistance groups. A second camera that was developed just before the war was the Riga Minox camera designed by Walter Zapp in 1936. Initially the minicameras were marketed for the public, but they were very quickly adopted for espionage purposes by intelligence and government agencies.

**Microfilms in espionage.** Microfilms were first used for espionage in 1859, and were later used to transport messages during the Franco-Prussian war of 1870 by carrier pigeon. However, they came to much more prominence in the 1920s for keeping copies of bank records and development of Recordak by Kodak. It was, however, during the Second World War when the microfilms flourished. They were used in regular military mail by the American forces to reduce the cost of shipping tons of mail. Microfilms were also the main way to photograph military installations and documents, as well as types and rates of weapons production. They were also used to transfer coded messages between the army and the intelligence agents behind enemy lines. Transport of the microfilms was not difficult due to their small size. Microfilms were, and still are, easily concealed in hollowed-out pencils, pens, cans, coins or other instruments smuggled by couriers across borders, and in many cases they remain a method of choice for espionage.

Microdots can be concealed even more easily than microfilms by being placed in a regular letter, under a stamp or in a dental filling. Microdots have also become



An American coin showing hidden microfilm. ©JEFFREY L. ROTMAN/CORBIS.

an anti-theft device: a Stoptheft microdot can be used to mark property.

*Photographic Resolution  
Rosenberg (Ethel and Julius) Espionage Case*

## ■ FURTHER READING:

### BOOKS:

Pritchard, Michael, and Douglas St. Denny. *Spy Camera: A Century of Detective and Subminiature Cameras*. London: Classic Collections, 1993.

White, William. *The Microdot: History and Application*. Williamstown: Phillips Publications, 1992.

### ELECTRONIC:

Minoxography Community. D. Scott Young and Ferry Ansgar. "A Brief History of Minox." <<http://www.minoxography.org/history.html>> (10 March 2003).

University of California. Southern Regional Library Facility. The history of microfilm: 1839 to present. December 3, 2002. <<http://www.srlf.ucla.edu/exhibit/text/BriefHistory.htm>> (10 March 2003).

### SEE ALSO

*DNA Sequences, Unique*

## Microphones

### ■ AGNIESZKA LICHANSKA

A microphone is a transducer that converts sound waves into electrical signals proportional to the strength of the sound. The microphone output can be recorded or transmitted.

Although there are various types of microphones, the operating principal is the same. A diaphragm, either metal or plastic, vibrates in response to a sound wave and transmits the movement to an electrical component causing an induction of an electrical current. Microphones can be classified according to the way the diaphragm transmits sound or the way they pick up the sounds.

Based on the way the sound is transmitted, there are five groups of microphones: carbon, dynamic, ribbon, condenser and crystal. Each of these microphones can be



U.S. Ambassador to the United Nations Henry Cabot Lodge, left, complains to the United Nations Security Council in 1960 about a wooden carving of the Great Seal of the United States in the office of the U.S. Ambassador in Moscow (shown) that had been implanted with a miniature listening device by the Soviets. AP/WIDE WORLD PHOTOS.

made to pick up sounds from various directions. There are omnidirectional, bidirectional, cardioid, hypercardioid, supercardioid and parabolic microphones. Omnidirectional microphones pick up sounds from the entire surrounding area (360°). In contrast, bidirectional devices have only a 90° pickup arc. The various cardioid microphones pick up sounds from a 105–131° arc. Parabolic microphones are the most unidirectional microphones, therefore, they have to be pointed directly at the source of sound. Their name comes from the fact the microphone itself (for example, omnidirectional) is surrounded by a parabolic dish. This dish gathers sounds and, by directing it to the microphone, also amplifies it.

None of the different types of microphones is superior to the other. They are all suited for different purposes. Important factors in selecting a microphone include the

sensitivity, quality of sound, overload characteristics, and, especially for surveillance and intelligence purposes, the size of the microphone.

The sensitivity of the microphone is measured by an amount of current produced. The currents produced by the microphones are very small and a signal has to be amplified before it can be used. However, amplification is not selective. Not only are the sounds amplified, but also any noise that was produced by an instrument itself. Sounds that are too loud or bad placement of a microphone can lead to distortion of the diaphragm known as an overload.

In any surveillance operation, placement of the microphone is crucial, not just for the quality of sound, but also for remaining inconspicuous. Microphones can also be carried by people to provide continuous surveillance or

rapid identification and response. Such microphones are often combined with a transmitter or a recorder to send or record conversations.

**Applications of microphones.** The most obvious application in security, surveillance, and espionage is to listen in on conversations. Microphones are combined with an amplifier to provide good sound quality. These sounds can be recorded or transmitted, depending on the situation or application of the microphone. They are used by individuals, police, security agencies, intelligence and counter-intelligence agents. The purpose is to monitor and identify the suspects, and obtain intelligence as to their plans and contacts.

The type of microphone used depends on the intended use. Parabolic microphones are used for distance surveillance as the best ones can pick up sounds from as far as 300 yards. However, most of these microphones can be easily blocked by an obstacle in the form of an object or person, causing poor sound quality or loss of sound reception. A solid wall or door would be impenetrable if it was not for a contact microphone that can intercept any audio signal through a solid material. The choices among microphones to be placed in a room or to be carried by a person are immense. A number of microphones built into pens are available. There are also microphones as small as a tiepin, allowing inconspicuous surveillance and spying.

Microphones are used as security devices alone or in combination with other instruments such as fingerprint scanners, retinal scanners or passwords, to secure access to high security areas or computers.

#### ■ FURTHER READING :

##### BOOKS:

White, Paul, ed. *Basic Microphones*. London: Sanctuary Press, 2000.

##### ELECTRONIC:

How Stuff Works. "How do microphones work, and why are there so many different types?" <<http://electronics.howstuffworks.com/question309.htm>> (6 March 2003).

Nave, C. R. Georgia State University (2000). <<http://hyperphysics.phy-astr.gsu.edu/hbase/audio/mic.html>> (6 March 2003).

SpyChest. Parabolic Microphone DetectEar <[http://www.spytechs.com/listen\\_voice\\_equip/detect\\_ear.htm](http://www.spytechs.com/listen_voice_equip/detect_ear.htm)> (6 March 2003).

Tan, P. Multimedia Bluffer's Guides. "Microphones" (1996). <<http://home1.pacific.net.sg/~firehzrd/audio/mics.html>> (6 March 2003).

UCSC Electronic Music Studios. Technical Essays. <[http://arts.ucsc.edu/ems/music/tech\\_background/tech\\_background.html](http://arts.ucsc.edu/ems/music/tech_background/tech_background.html)> (6 March 2003).

The University of Iowa. Multimedia Writing, Radio essays. <<http://twist.lib.uiowa.edu/radio/Resources.html>> (6 March 2003).

#### SEE ALSO

*Audio Amplifiers*  
*Laser Listening Devices*  
*Parabolic Microphones*

## Microscopes

The ability to view things that are too small to be seen by the unaided eye is important in espionage and security. For example, the diagnosis of an infection often relies in part on the visual examination of the microorganism. Information about how the microbe reacts to certain staining methods (e.g, the bacterial Gram stain), the shape of the microbe, and the reaction of antibodies to the microbe all provide important clues as to the identity of the organism.

As well, microscopic examination of documents can reveal information that cannot otherwise be seen. The high magnification and analysis of the elements that make up a sample that is possible using specialized techniques of scanning and transmission electron microscopy can reveal the presence of material that is of suspicious origin (i.e., missile casing), or the presence of codes on a surface.

A microscope is the instrument that produces the highly magnified image of an object that is otherwise difficult or impossible to see with the unaided eye. A microscope is able to distinguish two objects from one another that could not be distinguished with the eye. The resolving power of a microscope is greater than that of the eye.

**History of the microscope.** In ancient and classical civilizations, people recognized the magnifying power of curved pieces of glass. By the year 1300, these early crude lenses were being used as corrective eyeglasses.

In the seventeenth century Robert Hooke published his observations of the microscopic examination of plant and animal tissues. Using a simple two-lens compound microscope, he was able to discern the cells in a thin section of cork. The most famous microbiologist was Antoni van Leeuwenhoek. Using a single-lens microscope that he designed, Leeuwenhoek described microorganisms in environments such as pond water. His were the first descriptions of bacteria and red blood cells.

By the mid-nineteenth century, refinements in lens grinding techniques had improved the design of light microscopes. Still, advancement was mostly by trial and error, rather than by a deliberate crafting of a specific design of lens. It was Ernst Abbe who first applied physical principles to lens design. Abbe combined glasses that bent light beams to different extents into a single lens, reducing the distortion of the image.



The resolution of the light microscope is limited by the wavelength of visible light. To resolve objects that are closer together, the illuminating wavelength needs to be smaller. The adaptation of electrons for use in microscopes provided the increased resolution.

In the mid-1920s, Louis de Broglie suggested that electrons, as well as other particles, should exhibit wavelike properties similar to light. Experiments on electron beams a few years later confirmed this hypothesis. This was exploited in the 1930s in the development of the electron microscope.

**Electron microscopy.** There are two types of electron microscope. They are the transmission electron microscope (TEM) and the scanning electron microscope (SEM). The TEM transmits electrons through a sample that has been cut so that it is only a few molecules thin. Indeed, the sample is so thin that the electrons have enough energy to pass right through some regions of the sample. In other regions, where metals that were added to the sample have bound to sample molecules, the electrons either do not pass through as easily, or are restricted from passing through altogether. The different behaviors of the electrons are detected on special film that is positioned on the opposite side of the sample from the electron source.

The combination of the resolving power of the electrons, and the image magnification that can be subsequently obtained in the darkroom during the development of the film, produces a total magnification that can be in the millions.

Because TEM uses slices of a sample, it reveals internal details of a sample. In SEM, the electrons do not penetrate the sample. Rather, the sample is coated with gold, which causes the electrons to bounce off of the surface of the sample. The electron beam is scanned in a back and forth motion parallel to the sample surface. A detector captures the electrons that have bounced off the surface, and the pattern of deflection is used to assemble a three dimensional image of the sample surface.

**Scanning, tunneling, and other microscopy techniques.** In the early 1980s, the technique called scanning tunneling microscopy (STM) was invented. STM does not use visible light or electrons to produce a magnified image. Instead, a small metal tip is held very close to the surface of a sample and a tiny electric current is measured as the tip passes over the atoms on the surface. When a metal tip is brought close to the sample surface, the electrons that surround the atoms on the surface can actually "tunnel through" the air gap and produce a current through the tip. The current of electrons that tunnels through the air gap is dependent on the width of the gap. Thus, the current will rise and fall as the tip encounters different atoms on the surface. This current is then amplified and fed into a computer to produce a three dimensional image of the atoms on the surface.

Without the need for complicated magnetic lenses and electron beams, the STM is far less complex than the electron microscope. The tiny tunneling current can be simply amplified through electronic circuitry much like that used in other equipment, such as a stereo. In addition, the sample preparation is usually less tedious. Many samples can be imaged in air with essentially no preparation. For more sensitive samples that react with air, imaging is done in vacuum. A requirement for the STM is that the samples be electrically conductive.

Scanning tunneling microscopes can be used as tools to physically manipulate atoms on a surface. This holds out the possibility that specific areas of a sample surface can be changed.

Other forces have been adapted for use as magnifying sources. These include acoustic microscopy, which involves the reflection of sound waves off a specimen; x-ray microscopy, which involves the transmission of x rays through the specimen; near field optical microscopy, which involves shining light through an opening smaller than the wavelength of light; and atomic force microscopy, which is similar to scanning tunneling microscopy but can be applied to materials that are not electrically conductive, such as quartz.

#### ■ FURTHER READING:

##### BOOKS:

- Aebi, Engel. *Atlas of Microscopy Techniques*. San Diego: Plenum Press, 2002.
- Hayat, M. Arif. *Microscopy, Immunohistochemistry, and Antigen Retrieval Methods for Light and Electron Microscopy*. New York: Plenum Publishing, 2002.
- Murphy, Douglas, B. *Fundamentals of Light Microscopy and Electronic Imaging*. New York: Wiley-Liss, 2001.

##### SEE ALSO

*Biological Warfare*  
*Chemical and Biological Detection Technologies*

---

## Microwave Weaponry, High Power (HPM)

---

High-power microwave (HPM) weaponry sends out a short, extremely high-voltage burst of electromagnetic energy capable of disrupting computer systems for a fraction of a second. Although the disruption is short, the burst causes computers to reset, and if the computers operate something as sensitive as the control and navigation systems of a jet in mid-flight, the result could be lethal. HPM systems

are effective weapons by virtue of the fact that their use is difficult to trace. For technologically sophisticated powers such as the United States, however, HPM weapons are potentially as much of a threat as they are an asset.

**HPM capabilities.** If HPM simply shut down computer systems, that might be enough to make them formidable weapons, but their usefulness does not stop there. As anyone who has ever accidentally put a piece of metal in a microwave oven knows, metal in contact with microwaves tends to spark. If the conductive wire harness inside an airplane fuel tank were hit with a microwave near the end of a transoceanic flight, when the concentration of fumes in the tank is heavy, the result could be an explosion.

To further the threatening quality of HPM weaponry, these systems use “ammunition”—electromagnetic energy—that is invisible, travels at the speed of light, and exists in virtually limitless supply. Nor does an HPM beam leave any markings, like the spent round of a traditional weapon, that would connect it to the weapon that fired it.

**HPM uses.** Until the 1970s, HPM technology was impractical. Over the next two decades, however, developments in plasma physics, energy storage, and the technology of switching devices made these weapons systems viable around the time the Cold War came to an end. The Soviets invested more research in the field than did the West, a logical choice because HPM weaponry is more useful to the less technologically advanced side. The more sophisticated a nation’s weapons systems, and the more reliant on microprocessors, the more vulnerable these potentially are to HPM.

Russian authorities claimed that in 1995, Chechnyan rebels used HPM to subvert a Russian security system and gain entry to a restricted-access area. Four years later, the Russians maintained that United States forces used HPM weapons to disable Yugoslav communications during the North Atlantic Treaty Organization (NATO) campaign in Kosovo.

Carbon-graphite coils capable of generating an electromagnetic pulse used to destroy electronics equipment—especially communications equipment—can be fitted to cruise missiles. Carbon-graphite equipped cruise missiles were used by U.S.-led forces in raids on Baghdad, Iraq, in 1991 and in 2003.

Scientists at Lawrence Livermore National Laboratory also have developed an HPM weapon for the Department of Justice: aimed at a moving vehicle, the HPM could shut off the electronic ignition, thus bringing a high-speed car chase to an abrupt end.

American use of HPM systems carried with it the threat that enemies might gain access to such weapons as well. In view of this danger, the Department of Defense

took steps to “harden” the electronic circuitry of weapons to protect them against attacks.

#### ■ FURTHER READING:

##### PERIODICALS:

Arkin, William M. “‘Sci-Fi’ Weapons Going to War.” *Los Angeles Times*. (December 8, 2002): M1.

Epstein, Edward. “U.S. Has New Weapon Ready.” *San Francisco Chronicle*. (February 14, 2003): A1.

Fulghum, David A. “Microwave Weapons May Be Ready for Iraq.” *Aviation Week & Space Technology* 157, no. 6 (August 5, 2002): 24.

Kirkpatrick, Melanie. “Weapons with a Moral Dimension.” *Wall Street Journal*. (January 14, 2003): A15.

##### SEE ALSO

*E-Bomb*

*Electronic Countermeasures*

*Electronic Warfare*

*Radio Frequency (RF) Weapons*

---

## Middle East, Modern U.S. Security Policy and Interventions

---

#### ■ JUDSON KNIGHT

The Middle East figures heavily in U.S. national and international security policy. Factors include the existence of enormous oil reserves in several countries, U.S. support for Israel, and the proliferation of terrorism on the part of Palestinian, Arab nationalist, and Muslim fundamentalist organizations. Coupled with these three factors, the last of which became particularly significant as Mideast terrorism reached the United States itself in 1993, was a Cold War-era competition with the Soviet Union for influence in the region. This prompted the U.S. government to aid Afghanistan, a country low in natural resources, but high in strategic value. Later, in the war on terrorism, Afghanistan itself would become a venue for U.S. military action. Such realignments of policy have been a regular feature in U.S. policy, which has seen shifts in its approach toward Egypt, Iran, Iraq, and other countries in the Middle East over the years.

### Israel and the Rise of Terrorism

The defeat of the Ottoman Empire in World War I ended the last in a series of Turkish, Arab, and Persian empires

that had controlled the region for 13 centuries. Beginning in the 1920s, Turkey rapidly modernized under the leadership of Mustafa Kemal, also known as Atatürk. While maintaining its Muslim faith, Turkey eschewed traditions such as the denial of equal rights for women, and in the eyes of Westerners, served as a model for the region. After World War II, Turkey became a strategic ally and a member of the North Atlantic Treaty Organization (NATO).

In the decade after the end of World War II, new nations emerged from what had formerly been colonies and protectorates controlled by the United Kingdom, France, and other European powers. Some of these new nations, such as Iraq, formed from three Ottoman provinces, were a product of modern agreements, with little historical identity as a national unit. Such conditions created tension between the military, hereditary monarchs, and religious and ethnic groups.

## The Arab-Israeli Wars

Nowhere was the tension of the new Middle East more apparent than in the relationship between Israel and its Arab neighbors. A 1947 United Nations (UN) map divided the area today known as Israel almost equally between Israelis and Arabs. Dissatisfied with this proposal, and opposed to the establishment of an Israeli state, Egypt, Iraq, Jordan, and Syria attacked Israel shortly after its establishment as a nation in May 1948. Though outnumbered, the Israelis had a superior military, and defeated the Arab nations. As a result, Israeli territory expanded to encompass an area larger than that allotted in the original UN partition.

Israel attacked Egypt in 1956, as part of the Suez Canal crisis, but was forced back by pressure both from the United States and the Soviet Union. In March 1957, U.S. President Dwight D. Eisenhower proclaimed the Eisenhower Doctrine, whereby “the United States regards as vital to the national interest and world peace the preservation of the independence and integrity of the nations of the Middle East.” Up to this point, the Cold War lines in the Middle East were not sharply drawn, but as Egypt’s Gamal Abdel Nasser and other Arab leaders entered into agreements with the Soviets, the United States increasingly backed Israel.

In the Six-Day War of June 1967, Israel once again defeated a much larger force, and gained control of the west bank of the Jordan River, which had been Jordanian territory. From that point, the inhabitants of the West Bank gained a political identity not as displaced Jordanians, but as Palestinians. Soon Yasser Arafat and the Palestine Liberation Organization (PLO) would emerge as spokespeople for the Palestinians, but the groups that made up the PLO did not speak with words alone. During the years that followed, Palestinian and other groups

would conduct scores of terrorist attacks that killed hundreds of Israelis, Americans, and others.

**The 1973 War and Lebanon.** The fourth Arab-Israeli war began with a combined Egyptian and Syrian attack against Israel on October 6, 1973. Other Arab nations eventually sent forces as well. The Arabs were heavily supplied with Soviet arms and equipment, and in retaliation the United States on October 14 began resupplying Israel. On October 18, two days after the Israelis crossed the Suez Canal, the Organization of Petroleum-Exporting Countries (OPEC) announced a cutback in oil production. This raised gasoline prices, causing the first of several energy crises that dealt severe, if temporary, blows to the U.S. economy.

Though Israel would remain at odds with most of its Arab neighbors, events in 1977 and 1978 provided an opportunity for peace with Egypt. Egyptian President Anwar Sadat and Israeli Prime Minister Menachem Begin first conducted talks in late 1977, and in September 1978, President James E. Carter brought both leaders together for talks at Camp David. The Camp David accords provided hope for peace in the Middle East, but incited anger from militants in the Arab world; on October 6, 1981, a member of an Islamic fundamentalist group assassinated Sadat.

In 1978, Israel invaded southern Lebanon, and began a full-scale occupation in 1982. Also overrun by Syria, which sought to exercise control over the country, Lebanon descended into chaos. It was in this context that President Ronald Reagan sent U.S. forces into the capital city of Beirut, where in April and October 1983, two separate terrorist bombings killed a total of 259 Americans, including 242 Marines. Reagan withdrew the troops from Lebanon in 1984.

## Islamic Fundamentalism

Although U.S. support for Israel has remained one pretext among many cited by Middle East terrorists as justification for their attacks, the suicide bombers in Beirut were not directly linked with the Palestinian issue. Instead, they were members of a radical Shi’a Muslim group ultimately affiliated with Iran, where Islamic militants had taken control and established a fundamentalist, passionately anti-American theocracy in 1979.

One of the most successful early covert actions of the Central Intelligence Agency (CIA) was Operation AJAX, conducted against the regime of Iranian Prime Minister Mohammad Mossadegh in 1953. Mossadegh had seized control of the Anglo-Iranian Oil Company in 1951, whereupon the British Secret Intelligence Service (MI6) developed a plan for covert action against him. MI6 brought the CIA in on the plan in November 1952, and at the behest of CIA director Allen Dulles, Kermit Roosevelt acted as commander of the operations.

CIA and MI6 support for groups loyal to the deposed monarch, Shah Mohammad Reza Pahlavi, resulted in his

restoration to the throne in August 1953. Over the next 25 years, the shah remained a loyal U.S. supporter, and attempted to modernize his country, but accompanied that modernization with acts of repression. His secret police, SAVAK, operated throughout the country, practicing torture and dealing severely with opponents to the shah's rule.

By 1978, popular unrest had reached a boiling point, and the shah fled the country in January of the following year. Shi'ite fundamentalists led by the Ayatollah Ruhollah Khomeini declared Iran the world's first Islamic republic in February 1979. On November 4, militants seized control of the U.S. embassy in Teheran, taking 52 Americans hostage. The Carter administration secretly called on the U.S. military to make a response, and in April 1980, a team composed of personnel from special military units attempted a rescue.

The mission was aborted after a helicopter and transport plane crashed at a remote desert staging area, killing eight men. The incident marked a low point for the U.S. military, which had seen no significant action since the ceasefire in Vietnam seven years earlier, and it proved to be a major contributing factor in Carter's failure to win reelection. Reagan won in part because of promises to build up the military, and on the day of his inauguration in January 1981, Iran released the hostages after 444 days of captivity.

Even as these events were taking place in Iran, neighboring Afghanistan became a Cold War battleground with the Soviet invasion of December 1979. The action called for a U.S. response, but just what that response should be was not immediately clear. Direct U.S. intervention was not considered, and Carter chose economic sanctions, keeping U.S. athletes home from the 1980 Olympics in Moscow. This did little to sway the Soviets, and resulted in the Soviet boycott of the 1984 Games in Los Angeles.

Reagan, on the other hand, chose to supply the resistance, various tribal groups known collectively as the *mujahideen*, or "holy warriors." While Saudi Arabia provided funds, China provided weapons, and Egypt provided training, the United States supplied the group of approximately 100,000 insurgents with sophisticated weaponry. Most notable among these were Stinger anti-aircraft missiles, funded as part of a secret October 1985, congressional appropriation of \$470 million. The United States also provided a variety of antitank missiles, C-4 explosives, and even Soviet-made equipment such as Kalashnikov rifles, as well as medical supplies, food, and clothing.

**Iran-Contra and blowback.** U.S. support for the *mujahideen* was to prove a significant factor in bringing an end to the Soviet occupation of Afghanistan, which in turn helped bring down the entire Soviet empire. Despite this

salutary result, the success in Afghanistan had a number of less positive consequences as well. One of these, the Iran-Contra affair, may not have been so much a by-product as a concurrent event. In both cases, the United States secretly supported Islamic fundamentalists, with whom it had little commonality of aims, in support of objectives dictated by the Cold War.

The most devastating side effect of the Afghanistan war was a phenomenon known to intelligence and security experts as "blowback," or unintended consequences of a highly negative nature. Even after the Soviets began withdrawing in late 1988, Washington continued to send arms to the *mujahideen*, and did so until a late 1991 agreement with the Soviets to discontinue all activity in Afghanistan. With the Cold War over, Afghanistan lost its strategic importance, and the United States rapidly turned its attention elsewhere.

This left Islamic militants in possession of large weapons caches, and as the world community focused on other issues, various *mujahideen* factions began fighting amongst themselves. By 1996, moderate groups such as that of the celebrated rebel commander Ahmad Shah Massoud had been defeated by the Taliban, militant fundamentalists with support from neighboring Pakistan. The Taliban provided safe haven for terrorist groups, most notably Osama bin Laden's al-Qaeda network, and supported their activities with heroin sales.

These circumstances would culminate in a number of terrorist attacks by al-Qaeda and other groups with apparent links to training camps in Afghanistan: the 1993 World Trade Center bombing; the June 1996 attack on the U.S. military complex in the Khobar Towers, Dhahran, Saudi Arabia (an incident for which several groups have claimed responsibility); al-Qaeda's bombing of two U.S. embassies in Africa in August 1998; the attack on the USS *Cole* in Yemen in October 2000; and eventually the events of September 11, 2001.

## State-Sponsored Terror and the Wars with Iraq

In the war on terrorism, much of the U.S. effort would be directed against what the administrations of presidents William J. Clinton and George W. Bush identified as state sponsors of terror. Clinton launched attacks on alleged al-Qaeda facilities in Sudan and Afghanistan in August 1998, while Bush initiated Operation Enduring Freedom in Afghanistan on October 7, 2001, and Operation Iraqi Freedom on March 19, 2003.

Some critics suggested that Saudi Arabia should be considered a terror-sponsoring nation, since bin Laden and most of the September 11 terrorists were Saudi citizens, and the Saudis supported the Taliban and numerous terrorist groups in Palestine. However, the situation with

Saudi Arabia is more complex than almost any other U.S. relationship in the Middle East, including the alliance with Israel.

Because of Saudi Arabia's oil reserves, wealth, and influence in the region, U.S. officials have generally tolerated anti-American statements by Saudi leadership figures. During Operations Desert Shield and Desert Storm, as the United States prepared for and launched military actions against Iraq in 1990 and 1991, Saudi Arabia provided both funds and bases for the operation.

**Libya.** An example of the degree to which oil wealth contributes to strategic complications in the Middle East is Libya. With its desert location, a population much smaller than New York City, minimal industry, and lack of natural resources other than oil, the North African country would never have been a significant international player had it not been for the discovery of oil in the 1960s. Wealth from oil, however, served to finance a wide array of international adventures on the part of Muammar al-Qaddafi, who seized power in September 1969.

At one point, it was estimated that Qaddafi provided some form of support, ranging from funds to weapons to training facilities, for more than 50 terrorist groups. These included not only Muslim militants, such as those operating in the southern Philippines, but also the Irish Republican Army, the Red Army Faction in Germany, and the Japanese Red Army. The wide geographic and ideological range of Qaddafi's exploits, combined with the seemingly bottomless resources he poured into terrorism, made him a notable foe of Washington in the 1970s.

U.S. planes shot down two Libyan fighter aircraft over the Gulf of Sidra in 1981, and five years later, after receiving credible intelligence of Libyan involvement in a West Berlin discotheque bombing that killed a U.S. soldier, Reagan launched air strikes against Libya. Qaddafi was markedly less active after the April 1986 bombings, but in December 1988, he orchestrated the bombing of Pan American Airlines Flight 103 over Lockerbie, Scotland, which killed 259 people.

During the 1990s, Qaddafi's influence receded as the Libyan economy declined. Eventually, the terrorists associated with the Berlin and Lockerbie bombings were brought to justice, and Qaddafi even made attempts toward a rapprochement with Washington. An Arab nationalist in the Nasser mold, he found himself alienated amid the rise of Muslim fundamentalists such as those of al-Qaeda, and vigorously denounced the September 2001 attacks. On the other hand, in 2003, when the United States attacked the Iraq of Saddam Hussein—another Arab nationalist—he denounced the United States.

**Iraq.** During the Iran-Iraq war (1980–88), the United States gave most of its support to Iraq, which most of the outside

world perceived as the less troublesome of two contentious states. But when Iraq invaded neighboring Kuwait in August 1990, President George H. W. Bush, under the auspices of the United Nations and with international support, retaliated with Operation Desert Storm.

The Persian Gulf War resulted in the Iraqi withdrawal from Kuwait, the imposition of no-fly zones over much of the country, and a requirement that Hussein relinquish all weapons of mass destruction (WMD). But it also left Saddam in power. On April 14, 1993, Iraqi intelligence agents attempted to assassinate Bush (who was no longer president) during a visit to Kuwait. Two months later, the administration of William J. Clinton launched a cruise missile attack on the Iraqi capital of Baghdad.

Saddam Hussein continued to obstruct UN weapons inspection efforts, and eventually forced all inspectors out of the country, claiming that the team included U.S. and Israeli spies. The United States and United Kingdom then launched Operation Desert Fox (December 16–19, 1998), a bombing campaign against strategic sites in Iraq. Saddam allowed the weapons inspectors back in but, in the view of the United States, continued to deceive and evade efforts toward uncovering his WMD.

Some authorities held that Hussein had played a supporting role in the 1993 World Trade Center bombing, and after the 2001 attack, President George W. Bush identified Iraq as a major sponsor of terror, suggesting that the Iraqi leader had directly supported the perpetrators of that attack as well. When Hussein failed to relinquish what Bush maintained were significant caches of weapons of mass destruction, the U.S. launched Operation Iraqi Freedom in March 2003. The campaign proved successful, resulting in Saddam Hussein's removal and sending a powerful message to neighboring Syria and other known supporters of terrorist movements.

## ■ FURTHER READING:

### BOOKS:

- Lenczowski, George. *American Presidents and the Middle East*. Durham, NC: Duke University Press, 1990.
- Lesch, David W. *The Middle East and the United States: A Historical and Political Reassessment*. Boulder, CO: Westview Press, 1990.
- Nelson, Jonathan M. *Paths Not Taken: Speculations on American Foreign Policy and Diplomatic History, Interests, Ideals, and Power*. Westport, CT: Praeger, 2000.
- Richelson, Jeffrey T. *The U.S. Intelligence Community*, 4th ed. Boulder, CO: Westview Press, 1999.
- Rothkopf, David J. *The Price of Peace: Emergency Economic Intervention and U.S. Foreign Policy*. Washington, D.C.: Carnegie Endowment for International Peace, 1998.
- Williams, Mary E. *The Middle East: Opposing Viewpoints*. San Diego, CA: Greenhaven Press, 2000.

SEE ALSO

*ADFGX Cipher*  
*Africa, Modern U.S. Security Policy and Interventions*  
*Bush Administration (1989–1993), United States National Security Policy*  
*Bush Administration (2001–), United States National Security Policy*  
*Carter Administration (1977–1981), United States National Security Policy*  
*Clinton Administration (1993–2001), United States National Security Policy*  
*Delta Force*  
*Egypt, Intelligence and Security*  
*Enduring Freedom, Operation*  
*Engulf, Operation*  
*Iran, Intelligence and Security*  
*Iran-Contra Affair*  
*Iranian Nuclear Programs*  
*Iraq, Intelligence and Security Agencies*  
*Iraq War: Prelude to War (The International Debate Over the Use and Effectiveness of Weapons Inspections)*  
*Israel, Counter-terrorism Policy*  
*Iraqi Freedom, Operation (2003 War Against Iraq)*  
*Israel, Intelligence and Security*  
*Jordan, Intelligence and Security*  
*Kenya, Bombing of United States Embassy*  
*Khobar Towers Bombing Incident*  
*Kuwait Oil Fires, Persian Gulf War*  
*Lebanon, Bombing of U.S. Embassy and Marine Barracks*  
*Libya, Intelligence and Security*  
*Libya, U.S. Attack (1986)*  
*Pan Am 103 (Trial of Libyan Intelligence Agents)*  
*Persian Gulf War*  
*Saudi Arabia, Intelligence and Security*  
*Sudan, Intelligence and Security*  
*Suez Canal*  
*Syria, Intelligence and Security*  
*Turkey, Intelligence and Security*  
*USS Cole,*  
*USS Liberty*  
*World Trade Center, 1993 Terrorist Attack*  
*World Trade Center, 2001 Terrorist Attack*

general sits on the Department of the Army staff. Military police personnel are involved in law enforcement operations ranging from protecting school crossings and writing parking tickets to murder investigations and undercover drug stings.

Personnel at U.S. bases around the country and the world provide temporary confinement of service members charged under the uniform code of military justice (UCMJ). Assuming the individual is found guilty after trial in a military court, where he or she is represented by a member of the judge advocate general (JAG) corps, if the sentence warrants, the convicted will serve time at a federal facility such as Fort Leavenworth in Kansas.

In addition to the regular military police activities, several branches have special undercover contingents—for example, the Army Central Investigation Division (CID)—as well as corrections officers. Military police, known as MPs in the Army and Marines, are trained for combat, and are often involved in second or third waves of an invading force. Once a target area has been subdued, MPs will often undertake the preservation of order, and the MP commander will serve as effective leader of the area until replaced.

■ FURTHER READING:

BOOKS:

Wright, Robert K. *Military Police*. Washington, D.C.: Center of Military History, 1992.

PERIODICALS:

Dominique, Dean J. "Convoy Rat Patrol." *Army Logisticians* 34, no. 3 (May/June 2002): 36–37.

Flatter, J. R. "Military Police: A Force of Choice for the 21st Century MEU (SOC)." *Marine Corps Gazette* 81, no. 7 (July 1997): 36.

Warden, John A. III. "The New American Security Force." *Airpower Journal* 13, no. 3 (fall 1999): 75–91.

SEE ALSO

*DoD (United States Department of Defense) Law Enforcement, Responses to Terrorism*

## Military Police, United States

The U.S. military police are the law enforcement corps within each of the major services. The army has its Military Police Corps, the navy its Shore Patrol, the air force its Air Force Security Police, and the Marine Corps its Military Police. These forces are staffed almost entirely by military personnel, and are responsible for all the ordinary functions of a police force, as well as additional military duties.

Formal organization of military police in the United States dates back to the early twentieth century. Today the largest of the military police corps is, not surprisingly, that of the largest service, the Army, whose provost marshal

## MOAB (Massive Ordnance Air Burst Bomb)

In addition to its raw destructive power, the Massive Ordnance Air Burst bomb (MOAB) has become part of a



A Massive Ordnance Air Blast bomb, or MOAB, the largest conventional bomb in the U.S. weapons arsenal, is prepared for testing at Eglin Air Force Base, Florida, March 11, 2003. AP/WIDE WORLD PHOTOS.

military and intelligence effort to discourage and demoralize enemy forces. Upon detonation, MOAB produces a mushroom cloud similar to a nuclear blast. The MOAB bomb is the most powerful non-nuclear weapon in the U.S. arsenal.

At 21,000 pounds, the MOAB bomb is 6,000 pounds heavier than the next largest conventional bomb, the BLU-82 (nicknamed the “Daisy Cutter”) bomb used in Vietnam. Like the BLU-82, the MOAB is a fuel air disbursement bomb. In Vietnam the large blast from the BLU-82 was used to create instant landing zones for helicopters.

Although both the BLU-82 and MOAB are dropped from a B-52 or an MC-130 cargo plane flown by Air Force Special Operations Forces, the MOAB has a GPS based satellite guidance system to enhance accuracy. The BLU-82 has an estimated target error allowance of several hundred feet. In contrast, the MOAB was designed to guide to within one meter of its intended detonation point. This accuracy was important to planners in carefully calculating the radius of the fireball and destructive blast from MOAB.

Fuel air explosives are designed to explode above the ground, disperse aerosolized fuel, and then detonate the

highly volatile fuel-air mixture. The concussive detonation produces a violent shock wave.

BLU-82 bombs proved useful in attacking cave complexes in Afghanistan containing Taliban and Al Qaeda terrorists because the violent blast—in addition to its direct destructive force—also deprives those under the blast of oxygen.

The power of the blast is intended not only to kill and destroy—but also to shock and demoralize enemy troops. Discussing the bomb in March of 2003, Defense Secretary Donald H. Rumsfeld acknowledged the Pentagon’s plans to use MOAB to shock enemy troops in the impending war with Iraq and asserted, “There is a psychological component to all aspects of warfare.” Potential use of MOAB was incorporated by military planners into U.S. “shock and awe” tactical doctrine that calls for swift and intense military attacks to disorient enemy troops.

The United States Air Force conducted a demonstration test of the MOAB at Eglin Air Force Base near Pensacola, Florida, on March 11, 2003. Press coverage was extensive, and within hours of the test the Pentagon released footage of the blast to news services. Pentagon planners hoped that footage would make its way into Iraq

and help discourage Iraqi troops from what seemed to be futile resistance against a vastly superior U.S.-led coalition.

#### ■ FURTHER READING:

##### PERIODICALS:

Shanker, Tom. "Largest Conventional Bomb Dropped in a Test in Florida." *New York Times*. March 12, 2003.

##### SEE ALSO

*Enduring Freedom, Operation Vietnam War*

---

## Molecular Biology: Applications to Espionage, Intelligence, and Security

---

■ BRIAN HOYLE

Molecular biology involves the use of techniques to determine or rearrange the sequence of the components of deoxyribonucleic acid (DNA).

In the mid-1970s, it became possible, using what came to be called recombinant DNA technology, to splice a specific region of DNA from one organism into the DNA of another to express the protein that the insert coded for.

### Molecular biology and "weaponizing"

During the Cold War of the 1950s and 1960s, the consensus in the intelligence community was that the Soviet Union explored the use of recombinant DNA technology to engineer more lethal microorganisms for use as weapons. For example, one project attempted to insert the genetic coding for cobra and scorpion venom into the DNA of a bacteria that could enter the body.

Genetic engineering of bacteria, especially spore-forming types that are resistant to all known antibiotics, is another aspect of molecular biology that has been recognized as a military and national security threat. The infections caused by the engineered bacteria would be virtually impossible to treat. As well, genes that code for toxins could be transferred to spore forming bacteria such as *Bacillus anthracis* or *Clostridium botulinum*. Because the spores can survive for months, even years, in conditions that would kill the actively growing bacteria, the toxins would be more likely to harm an enemy.

To date, however, all indications are that such engineered bacteria do not exist. This may be because, for

example, antibiotic resistance is typically not due to the expression of a single gene. Rather, many genes need to be expressed, with their products operating coordinately, to bestow the resistance. Thus, the alteration of one or a few genes is, as of late 2002, unlikely to produce the resistant "superbug." As well, genetically engineered bacteria do not tend to survive well in the environment because there is an energy cost to the bacteria to express the inserted genetic material.

The military use of molecular biology to design biological weapons was banned by the 1972 Biological Warfare Convention. The signatory nations agreed in the 1980 and 1986 reviews of the convention that the ban applies to genetically engineered microorganisms. In the U.S., the Biological Weapons and Anti-Terrorist Act (1989) and the Antiterrorism and Effective Death Penalty Act (1996) prohibit the manufacture of biological weapons and the use of molecular techniques in these processes.

Rogue states and terrorist groups are unaffected by any such agreement. Thus, it has long been viewed as prudent to use molecular biological techniques to devise protective measures against genetically engineered microorganisms, and to conduct basic research on non-engineered, disease-causing microorganisms in order to devise vaccines or other treatments (i.e., rapid detection tests). The U.S. Army has utilized molecular biological techniques to study a variety of harmful bacteria and viruses since 1982 at their Fort Detrick, Maryland, laboratories (the Biological Defense Research Program). Other organizations have research programs as well (i.e., the Unconventional Pathogen Countermeasures Program run by the Defence Advanced Research Projects Agency; DARPA). The studies have involved determining the genetic basis of the infectious capability of microorganisms as well as the involvement of other components of the cell such as surface proteins.

**Molecular biology as an identification tool.** Since the 1970s, the techniques to extract target DNA (i.e. bacterial DNA) from the background DNA of all the other organisms in a sample has become refined and efficient. The ability to sequence even large segments of DNA can now be accomplished very quickly, largely because of the technology and computational power developed to allow the sequencing of the human genome. Finally, the DNA sequences of microorganisms that are serious health threats and are potential targets of bioterrorists have been determined (e.g., *Bacillus anthracis*, the bacterium that causes anthrax, and variola virus, which causes smallpox).

These developments make it possible to detect DNA sequences from certain bacteria and viruses. The technique known as the polymerase chain reaction (PCR) is critical to this aim. PCR enables a stretch of DNA to be amplified millions of times, to quantities that are detectable on electrophoretic gels or using DNA microchip technology, where the binding of a sequence of DNA that is a mirror image of the target sequence can be visualized.



The molecular approach can be used to distinguish one species of bacteria from another, even closely related species (i.e., *Bacillus anthracis* from *Bacillus subtilis*). A variety of enzymes exist that are capable of recognizing certain nucleotide sequences within the DNA and cutting the DNA apart at the sites where the sequence occurs. The result is fragments of differently sized DNA. The fragments can be separated according to their size using the technique of gel electrophoresis. The pattern of bands for one sample of bacteria that appears in the gel can be compared to the pattern given by another type of bacteria. If the patterns are identical, then the bacteria are the same species.

The enzyme digest technique can be combined with PCR to reveal even very small differences in DNA sequence. This allows sequences that are unique to a given bacterium to be detected. For example, this technique can identify *Bacillus anthracis* and *Yersinia pestis*, the bacterium that causes plague.

Molecular biology allows investigators to probe the cause of a disease outbreak. Learning the identity of the microorganism responsible for the outbreak can provide useful information as to the biological warfare capability of another country. For example, in 1979 an anthrax outbreak in the Soviet Union killed over 60 people. The cause was suspected of being the inhalation of anthrax spores that had been accidentally released from a military research facility. A team from the Los Alamos National Laboratory analyzed the DNA in preserved tissues of victims. At least five different types of *Bacillus anthracis* were found. A natural outbreak typically involves a single strain. The molecular evidence all but ruled out a natural outbreak.

Another area of active research is the development of molecular techniques to detect bacteria that can contaminate food. Naturally occurring bacteria such as *Salmonella typhosa*, *Campylobacter jejuni*, and *Escherichia coli* cause an estimated seven to 30 million cases of foodborne illness and up to 9,000 deaths every year in the United States alone. The economic losses and strain on the health care infrastructure have been identified as national security concerns.

**Molecular biology as an intelligence tool.** Molecular biology could potentially be used to encode information in DNA. Scientists have shown that by assigning letters of the alphabet and grammatical symbols to triplets of nucleotide bases, and then constructing a sequence within a DNA molecule, the sequence can yield a message when decoded by the recipient. In one study, DNA containing the coded message was spotted onto a period in a sentence of a letter and then sent through the mail. The recipient, aware of which symbol contained the DNA, extracted the DNA for sequencing, and from the sequence determined the hidden message. Only someone with knowledge of the existence of the DNA spot in the letter could receive the message.

Thus, molecular biology is poised to become an important means of transmitting information.

#### ■ FURTHER READING:

##### BOOKS:

Alberts, Bruce, Alexander Johnson, Julian Lewis, et al., eds. *Molecular Biology of the Cell*. New York: Garland Publishing, 2002.

##### PERIODICALS:

Clellenad, C.T., V. Risca, and C. Bancroft. "Hiding messages in DNA microdots." *Nature* no. 399 (1999): 533–534.

##### ELECTRONIC:

Los Alamos National Laboratory. "Tracing Biothreats with Molecular Signatures." *Research Quarterly*. Fall 2002. <[http://www.damtp.cam.ac.uk/user/gr/public/gal\\_milky.htm](http://www.damtp.cam.ac.uk/user/gr/public/gal_milky.htm)>(December 7, 2002).

##### SEE ALSO

*Biological Weapons, Genetic Identification*  
*DNA Fingerprinting*  
*Forensic Science*  
*Pathogen Genomic Sequencing*

---

## Moles

---

#### ■ JUDSON KNIGHT

A mole is a high-ranking intelligence officer for one agency who covertly feeds information to a rival or enemy agency. In practice, the difference between a mole and an agent-in-place—an employee of one intelligence agency who, of his or her own initiative, offers services to a rival or enemy agency—is a murky one, and seems to involve distinctions of rank. Moles are usually individuals who carry considerable authority within the agencies that employ them, and thus, the information they provide to their secondary employer is likely to be of high caliber.

In order to discuss examples of moles, it is necessary to draw distinctions between these and other categories of spy. Because high rank is usually regarded as a characteristic of a mole, most enlisted military personnel, such as the Marine guards at the U.S. embassy in Moscow during the 1980s, who were literally seduced into spying by attractive female KGB operatives, did not serve as moles, even though the intelligence they provided may have aided the services that used them as agents.

Furthermore, because moles are usually intelligence officers currently employed by the agency against which they are spying, the definition does not encompass all



Michael Raymond, right, is escorted from federal court in 1986 after being sentenced on a weapons charge and served with a Florida murder warrant. Raymond worked as an FBI “mole” uncovering political corruption in Chicago and New York in exchange for leniency. AP/WIDE WORLD PHOTOS.

members of the infamous Walker family spy ring, several of whom had retired from the U.S. Navy before they began spying for the Soviet Union. Most important, a mole is actively engaged in the covert collection and transfer of intelligence, meaning that inactive or sleeper agents, who are simply awaiting instructions before beginning work, do not qualify as moles.

## Soviet and Russian Moles

In the superpower conflict between the Soviet Union and the United States during the Cold War, and between the United States and the Russian Federation in the years since, there have been many more known cases of moles employed by the Soviets and Russians than by the Americans. This is most likely not a result of American failure to use moles as extensively; rather, unless they were caught, the identities of moles friendly to the United States are unlikely to be exposed until many years after the fact.

Among the most infamous Soviet moles in the West was the Cambridge spy ring, whose members included Harold (Kim) Philby, Donald Maclean, Guy Burgess, John

Cairncross, Anthony Blunt, and others. Recruited at Britain’s Cambridge University in the 1930s, these were scions of the privileged classes who had become disillusioned with the system that had fostered them. Beginning with Blunt, they readily provided information against their own nation and its allies, and recruited others to do so.

The members of the Cambridge spy ring for the most part, refused to accept pay for their deeds. This was not only because most of them came from wealthy backgrounds, but also because they genuinely considered that spying for the Soviet Union served an idealistic purpose. Actions of the Cambridge ring cost many lives, either directly or indirectly, and many of those identified by them died in situations involving torture. In the end, several members of the ring, including its leader Kim Philby, crossed the Iron Curtain and spent the remainder of their days under the care of their Soviet sponsors.

**Ideology and money.** In the ideologically charged atmosphere of the 1930s, and among an elite class such as that of the Cambridge spy ring, it was possible for the Soviets to find agents willing to serve as moles for ideological reasons and not for profit. By the end of World War II and the beginning of the Cold War, however, the pattern had changed: rather than ideology, money had become the principal motivating factor for most moles, who provided mostly technical rather than strategic information to their Soviet handlers.

From the standpoint of the Soviets, this later crop of moles was more reliable than the Cambridge ring and other ideological spies of the 1930s. A spy motivated by ideology fancies himself to be acting on moral principle alone, and thus, free to resist orders that he finds objectionable. By contrast, an individual so driven by greed that he will literally sell human lives for money is not likely to judge any job too dirty if the price is right.

Such was the case with Aldrich Ames of the Central Intelligence Agency (CIA), who provided the Soviets and later the Russians with information for nine years. At the time of his arrest in 1994, he was driving a late model red XJ6 Jaguar, just one of many items he had purchased with the \$2.7 million his handlers paid him over the course of the preceding decade. Much the same was the case with Robert Hanssen, a Federal Bureau of Intelligence counter-intelligence special agent who served as a mole for the Soviets and Russians prior to his arrest in 2001.

**A plethora of moles.** The Cambridge ring and the two paid moles of the 1990s are just a few among many examples of Soviet and later Russian infiltration directed against the United States or the West in general. In 1963, it was discovered that French diplomat George Pâques had been collecting intelligence on the North Atlantic Treaty Organization (NATO) and passing it on to the Soviets. Three years later, U.S. authorities arrested William Whelan, an army lieutenant colonel who served as intelligence advisor to the army chief of staff.

During this period, CIA counterespionage chief James Jesus Angleton spent considerable energy and resources on uncovering moles. During the late 1960s and early 1970s, Angleton conducted an aggressive “molehunt” in which more than 120 CIA agents came under suspicion. Quarrels with CIA chief William Colby led to Angleton’s dismissal in 1974. Yet, Angleton was not always inaccurate in his judgments; virtually from the moment he met Philby, an officer in British intelligence, he expressed suspicions that Philby was a mole—an assessment borne out by subsequent discoveries.

## U.S. and British Moles

The most well known mole for the West was Oleg Penkovsky, a colonel in the KGB. From the late 1940s, Penkovsky served the Soviet regime faithfully, but he became increasingly disillusioned with Communism in general and Premier Nikita Khrushchev in particular. Assigned to set up a KGB network while operating under the cover of a trade delegation, he first attempted to contact U.S. authorities, who initially refused to accept that the high-ranking officer would willingly provide them with secrets. Frustrated, Penkovsky offered his services to British intelligence through businessman Greville Wynne in 1961.

Wynne arranged a meeting with British intelligence in London, and thereafter Penkovsky supplied valuable information to both British and American authorities. Over an 18-month period, he delivered more than 5,000 photographs, as well as other information on Soviet military strength, war plans, missiles, and satellite systems. In the Cuban Missile Crisis of October 1962, President John F. Kennedy would make extensive use of information provided by Penkovsky. Afterward, the Soviets, aware that they had a mole in their midst, conducted a molehunt of their own. Several days after Penkovsky was tried and convicted in a 1963 show trial, he was executed by the KGB.

Another U.S. mole working in the Communist Bloc was Michael Goleniewski, a Polish military intelligence officer who passed secrets to the CIA before defecting to the West in 1960. Less fortunate was the case of Anatoly Filatov, caught in a CIA sex entrapment scheme in Algiers in 1976. Confronted with the threat of compromising revelations, Filatov agreed to provide the CIA with intelligence from the Soviet foreign ministry. Apprehended by the Soviets in 1978, he met the same fate as Penkovsky before him.

### ■ FURTHER READING:

#### BOOKS:

Buranelli, Vincent, and Nan Buranelli. *Spy Counterspy: An Encyclopedia of Espionage*. New York: McGraw-Hill, 1982.

Hood, William. *Mole*. New York: Norton, 1982.

Nash, Jay Robert. *Spies: A Narrative Encyclopedia of Dirty Deeds and Double Dealing from Biblical Times to Today*. New York: M. Evans, 1997.

Polmar, Norman, and Thomas B. Allen. *Spy Book: The Encyclopedia of Espionage*. New York: Random House, 1998.

Vise, David A. *The Bureau and the Mole: The Unmasking of Robert Philip Hanssen, the Most Dangerous Double Agent in FBI History*. New York: Atlantic Monthly Press, 2002.

West, Nigel. *Molehunt: Searching for Soviet Spies in British Intelligence*. New York: Berkley, 1991.

Wynne, Greville. *The Man from Moscow: The Story of Wynne and Penkovsky*. London: Hutchinson, 1967.

### SEE ALSO

*Ames (Aldrich H.) Espionage Case*  
*Cambridge University Spy Ring*  
*Cameras, Miniature*  
*Hanssen (Robert) Espionage Case*  
*Intelligence Agent*  
*Sex-for-Secrets Scandal*  
*United Kingdom, Intelligence and Security*  
*Walker Family Spy Ring*

## Monroe Doctrine

### ■ ADRIENNE WILMOTH LERNER

The Monroe Doctrine defined the U.S. position on international affairs involving nations in the Americas and former colonial holdings of European powers. In his seventh annual message to Congress on December 2, 1823, President James Monroe unveiled his plan for United States foreign policy. The United States government acknowledged the sovereignty of independent nations in the Americas, and declared the Americas closed to future colonization. The policy further stated that the United States would not be a party to European conflicts. The policy took decades to come to full fruition, receiving the name “Monroe Doctrine” in 1853. During the nineteenth century, the policy was tested during the Mexican-American and the Spanish-American Wars, though it was only directly invoked in the latter.

The Napoleonic Wars in Europe in the first decades of the nineteenth century stirred nationalist sentiment in both the Old and the New World. As European nations devoted increasing resources to combating Napoleon’s invading armies, they politically neglected their colonial holdings abroad. Nationalists in Latin America supported taking up arms against European colonial powers and establishing independent nations. Between 1815 and 1823, Argentina, Venezuela, Mexico, Peru, Colombia, and Chile

gained their independence and established republics. These fledgling nations needed, and sought, political recognition from larger, more influential nations. Knowing that they could not rely on the monarchist nations of Europe to support break-away democracies, the new American republics sought recognition from the United States.

In the United States, the European Napoleonic Wars spawned the War of 1812. British troops burned the U.S. capitol, but U.S. forces succeeded in routing British troops long enough to force a cease-fire and peace treaty. This second defeat of British forces more firmly established the United States as a thriving, independent nation, able to compete with European rivals. However, most members of the United States government sought to keep the nation out of European rivalries. When the revolutions in South America yielded new republics, the United States was left in a precarious position, caught between European and American interests.

A rumor circulated in diplomatic circles that the Holy Alliance of Russia, Austria, and Prussia was set to intervene on behalf of Spain in the colonial rebellions. In 1823, France invited Spain to restore the Bourbon monarchy with a promise of further aid against insurgent republics in the Americas. The monarchist alliance angered Great Britain, who was politically torn between the need to defend the principles of monarchist government, and keep the French from regaining strongholds in the Americas and the Caribbean.

British foreign minister George Canning lobbied the United States government to form an Anglo-American alliance to oppose the intervention of France or the Holy Alliance in Latin America. Many in the United States government supported the diplomatic move, but President Monroe and his Secretary of State, John Quincy Adams, were suspicious of the British plan. Adams advocated issuing a unilateral declaration, warning all European powers to refrain from joining colonial wars in which they had no direct involvement.

Monroe heeded Adams counsel. In a yearly speech, Monroe issued a statement proclaiming that any efforts to extend European political power in the Americas would be considered a threat to the security of the United States. Though the doctrine stated that the United States would refrain from participation in European conflicts, it left open the possibility for U.S. involvement in the Americas. Monroe counted on Britain to receive the statement as compromise, and recognize its mutual benefit. Indeed, the doctrine eventually worked largely because of backing from Britain.

The Monroe Doctrine was formally invoked seventy-five years later at the outbreak of the Spanish-American War. The United States cited Spain's continued involvement in Cuba as a threat to U.S. property and interests. The United States won the conflict against Spain, and in the years following the war, the United States acted to prevent European nations from collecting debts from

defaulting Latin American nations and former colonial holdings. When the Dominican Republic was bankrupt in 1904, United States President Theodore Roosevelt issued the Roosevelt Corollary to the Monroe Doctrine, stating that the United States could preemptively act to ward off European aggression in the Americas.

#### ■ FURTHER READING:

##### ELECTRONIC:

The Avalon Project at Yale University. *The Monroe Doctrine, 1823*. <<http://www.yale.edu/lawweb/Avalon/Monroe.htm>> (April 2003).

---

## Morocco, Intelligence and Security

---

Morocco gained its independence from France in 1956. The nation, strategically located in western North Africa, close to the Straits of Gibraltar, has long served as the gateway between Africa and Europe. After gaining its independence, Morocco sought to expand its borders and assert its control over various international interests in the region. Morocco was granted control of the internationalized trade city of Tangiers, but a long-standing dispute continues over its occupation of Western Sahara.

Morocco has suffered waves of political turbulence since its founding, but political reforms over the last decade have somewhat stabilized the region. With the recent rise of Islamist extremist groups in North Africa, the Moroccan government has sought to minimize the political impact of such groups in Morocco.

Morocco maintains specially trained military commando and intelligence units that focus on protection of national interests within Morocco, especially in the Western Sahara region. The main government intelligence agency is the *Direction de la Surveillance du Territoire* (DST), or Directorate of Territorial Surveillance. The DST conducts most all of Morocco's intelligence operations, both foreign and domestic. The largest organizational department of the DST is the counter-intelligence unit. Though the DST is known as both an intelligence agency and a secret police force that sometimes carries out political espionage, the agency does conduct joint operations with allied foreign intelligence services.

The Moroccan intelligence community has aided United States and British efforts to stem the spread of the al-Qaeda terrorist network. Surveillance operations carried out by the DST have led to the arrest of several suspects and the seizure of money and weapons destined

for terrorist cells in Europe or North Africa. Despite this cooperation with international anti-terrorism efforts and ongoing government reforms Morocco's intelligence and security services remain closely monitored by some organizations. Human rights organizations criticize the Moroccan intelligence community for the arrest, detainment, and torture of political dissidents, especially between 1960 and 1980.

#### SEE ALSO

*Terrorist and Para-State Organizations*  
*Terrorist Organizations, Freezing of Assets*

## Mossad

■ JUDSON KNIGHT

Israel's principal agency for intelligence collection, counterterrorism, and covert action is the Institute for Intelligence and Special Tasks, best known as Mossad, an abbreviation of its Hebrew name, ha-Mossad le-Modiin ule-Tafkidim Meyuhadim. In a tiny country surrounded by foes, the Mossad has been extremely active ever since its establishment in 1951. Its successes include the capture of former Nazi leaders, most notably Adolf Eichmann, as well as numerous triumphs of intelligence-gathering that contributed to Israeli victory in the 1967 Six-Day War. Mossad also conducted the legendary raid at Entebbe, Uganda, in which it rescued the passengers and crew of a French jetliner hijacked by Palestinian terrorists. Yet, Mossad has often come under criticism for perceived excessive actions against Israel's many enemies.

### History

David Ben-Gurion, Israel's first prime minister, established Mossad as ha-Mossad Letaum (the Institute for Coordination) on April 1, 1951. Mossad had a checkered record in its first decade. On the positive side, it was the first intelligence agency to capture a copy of Soviet leader Nikita Khrushchev's February 1956 "Secret Speech," in which he denounced the crimes of Josef Stalin before the 20th Party Congress. Mossad also ran several key operations in Arab lands, with Wolfgang Lotz in Egypt and Eliahu Cohen in Syria.

The Syrians eventually exposed Cohen, however, and hanged him in Damascus Square, while the Egyptians captured, tortured, and imprisoned Lotz in 1964. Meanwhile, another operative in Egypt, David Magen, turned out to be a double agent, and the work of Avraham Dar in Egypt during the mid-1950s ended in a disaster for Israeli intelligence, with numerous agents captured and imprisoned. At least one apparent success of this era turned out



Ephraim Halevy, in the first public address by a head of Mossad, speaks in Herzliya, Israel in 2000. AP/WIDE WORLD PHOTOS.

to be a political failure when Ben-Gurion reversed Mossad efforts to intimidate West German scientists who were assisting the Egyptians. Eager to develop better relations with West Germany, Ben-Gurion dismissed Mossad director Isser Harel (1952–63), who he had once accorded the title *Memuneh*, "the one in charge."

**1960s and 1970s.** Mossad, which gained its present name as the Institute for Intelligence and Special Tasks in 1963, fared much better in the 1960s. Joint operations with Shin Bet, the internal security force, led to the capture of Eichmann—who had overseen the murder of millions of Jews during the Holocaust—from his hiding place in Argentina. Under the leadership of Meir Amit (1963–68), Mossad focused on intelligence-gathering, which greatly aided Israeli military efforts in 1967. During this period, Mossad also assisted the defection of an Iraqi airman who delivered to Israel a Soviet MiG-21 fighter jet in 1963. In 1968, Mossad successfully captured eight missile boats that Israel had ordered from France, but which President Charles de Gaulle had placed under embargo. That year also saw the capture of nuclear technician Mordechai Vanunu, who had revealed Israeli nuclear secrets to the British press.

Following the massacre of Israeli athletes by the Palestinian terrorist group Black September at the Munich Olympics in 1972, Mossad directed an assassination effort

under an action team dubbed “the Wrath of God” (WOG). Over the next two years, WOG tracked down and killed more than a dozen members of Black September, but also accidentally killed a Moroccan waiter who had no affiliation with the terrorist group.

Failure to predict Egyptian actions leading to the Yom Kippur War in 1973 forced the resignation of several top officers, including Mossad director Zvi Zamir (1968–74). Yet, on July 3–4, 1976, Mossad more than recovered its reputation with the daring raid at Entebbe, codenamed Operation Thunderbolt. After intensive intelligence-gathering at the site, the Israelis assaulted the plane, rescuing all but four of its 97 passengers and losing a single officer—along with 20 Ugandan soldiers—in the process.

**1980s and 1990s.** During the 1980s, Mossad’s intelligence-gathering against Arab countries helped pave the way for Israeli airstrikes against Palestine Liberation Organization (PLO) headquarters in Tunisia, and against an Iraqi nuclear reactor. In April 1988, a Mossad assassination team infiltrated the residence of Abu Jihad, deputy to PLO chief Yassir Arafat, and killed him. Two years later, in March 1990, another hit team killed Gerald Bull, a Canadian scientist aiding the Iraqi weapons program, at his apartment in Brussels.

Among the less successful activities of Mossad during the 1980s and 1990s was its involvement in the Iran-Contra affair, when it acted as an intermediary between the United States and Iran. Embarrassment surrounding the failure of Mossad to prevent the assassination of Prime Minister Yitzhak Rabin by an Israeli citizen in November 1995 led to the resignation of Mossad director Shabtai Shavit in 1996. Prime Minister Shimon Peres then appointed Major General Danny Yatom, the first Mossad chief ever publicly identified. In 2000, Mossad undertook a recruitment campaign, complete with newspaper advertisements and a Web site that took applications on line.

## Organization and Operations

From its headquarters in the Israeli capital of Tel Aviv, Mossad oversees a staff estimated at approximately 1,200 personnel in the mid-1990s. It is assumed to consist of eight departments, of which the largest is Collections, tasked with espionage overseas. Officers in the Collections Department operate under a variety of covers, some diplomatic. The Political Action and Liaison Department is responsible for working both with allied foreign intelligence services, and with nations that have no normal diplomatic relations with Israel.

Among the departments of Mossad is the Special Operations Division or Metsada, which is involved in assassination, paramilitary operations, sabotage, and psychological warfare. Psychological warfare is also a concern of the Lohamah Psichlogit Department, which conducts propaganda and deception activities as well. Additionally, Mossad has a Research Department, tasked

with intelligence production, and a Technology Department concerned with the development of tools for Mossad activities.

### ■ FURTHER READING:

#### BOOKS:

- Eisenberg, Dennis, Uri Dan, and Eli Landau. *The Mossad Inside Stories: Israel’s Secret Intelligence Service*. New York: Paddington Press, 1978.
- Eshed, Haggai. *Reuven Shiloah: The Man Behind the Mossad: Secret Diplomacy in the Creation of Israel*. Portland, OR: F. Cass, 1997.
- Horesh, Joshua. *An Iraqi Jew in the Mossad: Memoir of an Israeli Intelligence Officer*. Jefferson, NC: McFarland & Co., 1997.
- Thomas, Gordon. *Gideon’s Spies: The Secret History of the Mossad*. New York: St. Martin’s Press, 1999.
- Westerby, Gerald. *In Hostile Territory: Business Secrets of a Mossad Combatant*. New York: HarperBusiness, 1998.

#### SEE ALSO

*Assassination*  
*Egypt, Intelligence and Security*  
*Eichmann, Adolf: Israeli capture*  
*Israel, Counter-terrorism Policy*  
*Israel, Intelligence and Security*  
*Middle East, Modern U.S. Security Policy and Interventions*  
*Palestinian Authority, Intelligence and Security*  
*Syria, Intelligence and Security*

## Motion Sensors

### ■ LARRY GILMAN

In security applications, a motion sensor is a device that detects human presence, usually inside a building or in the immediate vicinity of a building. Not all devices classified as “motion” sensors actually sense motion; for instance, passive infrared systems (PIRs) detect the infrared light (heat radiation) emitted by human beings. “Presence detectors” might be a more accurate term for this class of devices.

The simplest type of motion sensor sets up a circuit or closed electrical path partly composed of a beam of light. This beam is directed across an open space to be monitored to a photoelectric detector, which converts the incident light beam to a voltage signal; any interruption in the beam is detected as an interruption in the voltage signal. This straightforward design, still in use, has the disadvantage of monitoring only the space occupied by the beam itself. This means that several beams must be used to secure a doorway or passageway, and many beams must be used to monitor a large, complex space (e.g., armory).

Further, a beam-circuit system cannot distinguish between intruders of different sizes; a moth can interrupt a beam as effectively as a leg.

PIRs are also commonplace. Low-grade PIRs are often used for automatic lights, while more complex models are used for building security. PIRs do not detect motion, as mentioned above, but relatively rapid changes in the overall amount of infrared light in a scene. Slow, overall changes in the amount of infrared light, such as would occur when the sun goes behind a cloud or a room heats up, should not trigger the sensor; the sudden change caused by a human being entering the sensor's field of view should trigger the sensor. PIR sensors can fail to detect intruder movement that is (a) primarily towards or away from the sensor, rather than across its field of view, or (b) slow.

PIRs are passive because they detect energy that the scene emits of its own accord. Active motion detectors, in contrast, illuminate the scene with laser light, ultrasound (sound waves pitched too high for the human ear to detect), or microwaves (radar). Regardless of the type of energy used to illuminate the scene, there are two basic ways of using reflected energy to detect presence or intrusion: (1) monitor for relatively rapid changes in wave energy reflected from the scene, and (2) monitor for Doppler shifts in wave energy reflected from the scene. A Doppler shift is a change in frequency of a wave that is reflected from or emitted by a moving object or is measured by a moving observer. As in the motion-detection case, the detector is stationary, any frequency shift in waves reflected from the scene must result from the motion of objects in the scene.

Both PIRs and active detectors overcome the inability of the beam-circuit detector to distinguish between a tiny intruder and a large one, as these detector types can be set to trigger a light, door, alarm, or other device only if a certain threshold in signal intensity is crossed. However, there is no one, correct threshold. When designing a system to detect intrusion or presence, one wishes to avoid both a high false-alarm rate (which will over activate lights or doors or, in the case of a security system, eventually cause human operators to ignore the system) and a high likelihood of real presence detection. Yet, these two goals are in opposition; an insensitive detector will fail to detect persons that enter its field of view, but a too-sensitive detector will detect not only intruders, but also insects, vibrations in its mounting bracket, and other causes of minor signal variation. A compromise sensitivity must be chosen for each device type and application.

A more complex but potentially more informative class of motion-detection systems applies computer analysis to video images. By looking for changes from one image frame to the next, a computer can easily detect motion in a scene; the difficulty is to design algorithms that can distinguish between important motion (a man climbing a fence) and unimportant motion (leaves rustling in trees, cloud-shadows moving over the ground, etc.). A reliable video-based motion-detection scheme, therefore,

requires the application of artificial intelligence techniques. Such systems are under development, but not yet widely deployed.

## ■ FURTHER READING:

### BOOKS:

Lester, Andrew J., and Clifton L. Smith. "Analyses of Performance of Volumetric Intrusion Detection Technologies." Proceedings, 33rd Annual International Carnahan Conference on Security Technology. Oct. 12–14, 1999: 111–58.

---

## Mount Weather

---

Mount Weather, Virginia, is one of the United States Continuity of Government (COG) safety sites, though its exact COG functions are undisclosed. In the event of a national disaster that threatens normal government operations in Washington, D.C., facilities in locations such as Mount Weather are used to coordinate vital national operations. The facility is currently managed by the Federal Emergency Management Agency (FEMA) and is the home of the National Emergency Coordinating Center. The center manages FEMA operations after natural disasters and trains emergency management personnel. Though FEMA agents mostly handle more localized natural disasters, such as floods, hurricanes, or tornadoes, personnel are also trained to handle terrorist and massive attack scenarios.

The 434-acre mountain area that became Mount Weather was acquired by the National Weather Bureau (later, National Weather Service) in 1893. The bureau used the site to launch weather balloons and conduct atmospheric research. In the decades preceding World War I, the Weather Bureau monitored a series of kite stations on the site. The Army created an artillery range on the site at the outbreak of war in Europe in 1914. In 1936, the government granted Mount Weather to the Bureau of Mines. A series of tunneling experiments revealed that the mountain had an extremely dense and stable rock composition favorable to extensive tunnel construction. Recognizing the importance of such a site within a short distance of the national capital, the government restricted use of Mount Weather and planned to build a series of underground bunkers. Construction on the site was halted by World War II.

Amidst Cold War tensions, the government took a renewed interest in Mount Weather. In 1954, the Bureau of Mines began construction on the site's network of tunnels and underground rooms. Soon after construction started, security concerns prompted the government to shift control of the project to the military and the Army Corps of

Engineers finished construction of the subterranean facility in 1958. The facility was named “High Point” and was maintained as a shelter for government officials in the event of an attack on Washington, D.C. The underground structure contains offices, sleeping quarters, a hospital, independent water, sewage, and power systems, and radio, television, and computer networks. Estimates on its capacity vary, but Mount Weather is assumed to be able to support over 200 residents for one month.

FEMA was granted control of the premises in 1979, but much of the facility remains classified. FEMA’s above-ground facility serves as a command base for its national all-hazards operations. The communication networks located in the underground structure are part of the Emergency Broadcasting System, the national emergency alert system. The Resource Interruption Monitoring System (RIMS) tracks daily function and activity of vital national resources such as power systems and oil reserves. The Contingency Impact Analysis System (CIAS) creates and directs simulations of emergencies for training and readiness assessment purposes.

The largest operational center on the site is the FEMA Mount Weather Assistance Center. The center administers FEMA’s aid operations and often processes calls regarding aid requests and claims immediately following a disaster. While regional FEMA offices are equipped to handle most emergencies, the Mount Weather site is frequently active as a reserve operations post for disaster mitigation. Though FEMA continues operations on the site, the Continuity of Government emergency plan and facilities at Mount Weather have only been activated on two occasions. The first full-scale activation occurred during the Northeastern power blackout of November 9, 1965. More recently, some Mount Weather COG measures were set in motion after the September 11, 2001, terrorist attacks.

A government initiated expansion and renovation of many Mount Weather facilities began in 2001.

■ FURTHER READING:

ELECTRONIC:

Federal Emergency Management Agency. Mount Weather Emergency Assistance Center homepage. <<http://www.fema.gov/pte/weather.htm>>(November 20, 2002).

SEE ALSO

*Continuity of Government, United States Emergency Response Teams*

## Movies, Espionage and Intelligence Portrayals

■ JUDSON KNIGHT

Although depictions of espionage, intelligence, and related activities in motion pictures have not always tended toward realism, the movies’ portrayals of covert operations have to an extent mirrored events in the real world. Through the end of World War II, the activities depicted usually involved Nazis, but by the late 1950s, Hollywood had entered the Cold War espionage genre. Later decades have seen portrayals of terrorism and counterterrorism, as well as intelligence and security operations in futuristic settings. From the 1960s onward, the James Bond movies and other films and television shows have given increasingly whimsical treatments to covert operations. Hence it is ironic that some of what seemed like fanciful spy technology in the Bond movies of another time is now standard equipment, in some cases even within the civilian sector.

### From World War I to the Cold War

As early as 1918, with *I Want to Forget* (starring Evelyn Nesbit, whose involvement in a real-life murder drama would be depicted many years later in the book and film *Ragtime*), Hollywood set out to portray spies in film, but most early attempts were less than successful. Pre-World War II films on espionage tended to focus on the romantic and dramatic associations, and offered little in the way of authenticity.

Most authentic among the depictions of espionage in this era were the films of Alfred Hitchcock, whose most well-known espionage thrillers of the prewar era included the first version of *The Man Who Knew Too Much* (1934) and *The 39 Steps* (1935). These films established a theme that would become a fixture of spy movies thenceforth: the non-spy who stumbles into the middle of a conspiracy and is caught up in events he or she does not fully understand. Usually the non-spy ends up providing a key solution or otherwise outsmarting intelligence professionals—a resolution drawn from fantasy rather than real life.

**World War II.** As World War II began, Hitchcock released *Foreign Correspondent* (1940). The war years featured numerous films depicting Nazi, Japanese, and Allied espionage, and in this era before the establishment of the Central Intelligence Agency (CIA), the spy-hunters were usually special agents in the Federal Bureau of Investigation (FBI).

The era also saw one of the first movies to offer a humorous treatment of espionage: *They Got Me Covered* (1943), in which Bob Hope and Dorothy Lamour teamed





A War Room conference scene from “Dr. Strangelove, or: How I Learned to Stop Worrying and Love the Bomb,” a 1964 movie satirizing Cold War tensions among nuclear superpowers. ©THE KOBAL COLLECTION.

up as a pair of amateur spy-hunters chasing Nazis in Washington, D.C. More accurate portrayals of espionage in World War II—e.g., *The Man Who Never Was* (1956) and *Eye of the Needle* (1981, based on a Ken Follett novel of the same title)—had to wait until after the war was over.

A rare exception to the less-than-serious treatment of espionage during the war years actually appeared at the very beginning of the war: Warner Brothers’ *Confessions of a Nazi Spy* (1939), starring Edward G. Robinson. As Michael E. Birdwell’s 1999 book *Celluloid Soldiers* attested, Jack and Harry Warner were the first major figures in Hollywood to address Nazism, and at a time when the United States remained isolationist, this made *Confessions* a controversial film. According to Birdwell, members of the cast and crew received threats during production, and upon its release, the U.S. Senate called for an investigation of “war-mongering propaganda.” Ironically, hearings began in October 1941, just two months before America entered the war against Germany.

**The early Cold War period.** Espionage movies, like espionage itself, especially flourished in the Cold War era. Such films as *The Iron Curtain* (1948) and *The Third Man* (1949),

with a screenplay by Graham Greene, gave early notice of the high quality of the portrayals. This high quality continued throughout the early Cold War era, with offerings that included *Our Man in Havana* (1959, with a screenplay by Greene adapted from his novel); *The Manchurian Candidate* (1962), based on a Richard Condon novel involving brainwashing in the Korean War; and *The Spy Who Came in from the Cold* (1965), from a John Le Carré novel.

Hitchcock easily made the move to Cold War espionage with works such as his remake of *The Man Who Knew Too Much* (1955), now in a Cold War setting with James Stewart. *North by Northwest* (1959) returned to the theme of the innocent—played in this case by Cary Grant—caught in the middle of a vast international conspiracy. The title of a less well-known, but still critically acclaimed Hitchcock offering from this era, *Torn Curtain* (1966), with Paul Newman and Julie Andrews, refers not to a piece of fabric, but to the iron curtain.

## James Bond and the Marriage of Humor, Fantasy, and Espionage

By the late 1950s, depictions of espionage had reached a point at which filmmakers and TV producers could take an

entirely different approach. Instead of portraying covert action with the utmost of seriousness, these activities became fodder either for comedy or outlandish fantasy with a comedic twist. No greater example of this trend existed than James Bond, hero of 14 novels by Ian Fleming, himself a British intelligence officer.

Bond, Agent 007 in British intelligence, has a license to kill, and he uses that license—along with the audience’s willful suspension of disbelief—to the utmost in his endless operations against the Soviet-style organization known as Smersh. Whereas the Bond of Fleming’s books has a cerebral, serious quality, on screen his exploits are so outlandish as to be comical—and intentionally so. As unbelievable as Bond’s ability to come away unscathed from every adventure are his seemingly endless seductions of beautiful women, none of whom make any serious emotional demands on him, although several do try to kill him.

For all their apparently unrealistic qualities, the Bond films draw on elements of reality. Smersh was a real Soviet organization, founded by Josef Stalin, and the use of the initial “M” for Bond’s boss is a play on the “C” used to designate real-life heads of MI6, the British Secret Intelligence Service. Another figure with an initial for a name, “Q,” serves a function not unlike that of the Directorate of Science and Technology at the CIA.

It is Q’s job to supply Bond with technologically sophisticated, extremely efficient gadgetry designed to help him meet any challenge. These gadgets are a key feature of the Bond movies, and of other espionage films and TV shows in later years, such as *Mission: Impossible* and *Get Smart*. Many of the devices that seemed otherworldly in the 1960s—wireless telephones, films on silver discs, and computers small enough to fit into the palm of one’s hand—are part of everyday life today.

The first Bond book became *Casino Royale* (1953), with David Niven as Bond, but the true Bond film canon begins with *Dr. No* 10 years later. The movie was the first in the series to feature Sean Connery, the actor most widely praised for his portrayals of Bond, and it introduced the first of many beautiful “Bond girls,” Ursula Andress. With sexual liberation on the rise, and feminism still lagging behind at that time, subsequent Bond films featured numerous gorgeous sidekicks, seduced by Bond, only to be conveniently eliminated at some point, leaving the hero free to seek further partners in a future adventure.

Connery perfected his Bond persona over the course of four more movies in the 1960s: *From Russia, with Love* (1963), *Goldfinger* (1964), *Thunderball* (1965), and *You Only Live Twice* (1967). Fashion model George Lazenby took over the Bond role in *On Her Majesty’s Secret Service* (1969), but proved to be the least critically and popularly successful of all Bonds. Connery played Bond a fifth time in *Diamonds Are Forever* (1971).

The next five Bond movies featured Roger Moore: *Live and Let Die* (1973), *The Man with the Golden Gun* (1974), *The Spy Who Loved Me* (1977), *Moonraker* (1979),

and *For Your Eyes Only*. The last was released in June 1983, four months before Connery reappeared in a low-budget, critically panned final Bond performance, *Never Say Never Again* (1983). After Moore played Bond a sixth and final time in *A View to a Kill* (1985), Timothy Dalton took over in *The Living Daylights* (1987).

At this point, producers had expended all novels, screenplays, and treatments by Fleming, who died in 1964. The first Bond film that did not feature Fleming’s work was *Licence to Kill* (1989), also starring Dalton. The franchise went silent for six years, then revived in the mid-1990s with a series of films starring Pierce Brosnan as Bond: *Golden Eye* (1995), *Tomorrow Never Dies* (1997), *The World Is Not Enough* (1999), and *Die Another Day* (2002).

Cold War reality also mingled with humor in the black comedy *Dr. Strangelove; or, How I Learned to Stop Worrying and Love the Bomb* (1964). Peter Sellers impersonated both United States and Soviet leaders in the doomsday film, which culminates in an inadvertent global thermonuclear war.

**Television, fantasy, and humor.** Simultaneous with the heyday of Bond movies in the 1960s was the advent of television shows with an approach to espionage that was either fantastic, humorous, or both. Among these were the *The Avengers*, which debuted in 1961; *The Man from U.N.C.L.E.* (1964); *Get Smart* (1965), which, like *U.N.C.L.E.* and Bond, was heavy on gadgetry, with another Smersh-like enemy called CHAOS; *The Wild Wild West* (1965), which cleverly backdated modern intrigue and technology, setting them in the old West; *I Spy* (1965), the first television show featuring an African American star, Bill Cosby; *Mission: Impossible* (1966), which sometimes bordered on a serious portrayal of special operations, and which spawned two films starring Tom Cruise in the 1990s; and *The Prisoner* (1967).

The comedic is a recurring element of espionage films of the 1970s and beyond, including *The In-Laws* (1979), which was remade in 2003; *Dead Men Don’t Wear Plaid* (1982), with Steve Martin; a number of Leslie Nielsen movies, in which Nielsen plays a bumbling intelligence or law enforcement officer; and *True Lies* (1994), which mixes a semi-serious portrayal of an organization akin to the CIA with comedic touches, courtesy of Tom Arnold and Arnold Schwarzenegger.

Particularly successful have been the film series spawned by two 1997 espionage spoofs. *Austin Powers: International Man of Mystery*, in which Mike Myers plays an unlikely James Bond figure, led to two sequels, and *Men in Black*, starring Tommy Lee Jones and Will Smith, has had one. The latter series plays off of conspiracy theories concerning U.S. intelligence and studies of unidentified flying objects (UFOs) in the late 1940s and beyond, taking as its premise the idea that the UFOs actually

were alien spacecraft—a fact that the government has concealed from the populace.

The period from the 1970s onward has seen an ever-expanding variety of films that treat espionage, intelligence, special operations, or terrorism. Notable early examples from this period include *The Day of the Jackal* (1973), *The Conversation* (1974), and *Three Days of the Condor* (1975). Some other critically or popular acclaimed films have included *Another Country* (1984), about the formative years of British turncoat Guy Burgess; *Terminator* (1984) and *Terminator 2* (1991), with Schwarzenegger as an assassin from the future; and *Proof of Life* (2000), in which Russell Crowe plays an undercover operative in the private sector who rescues hostages from terrorist kidnappers.

As time has gone on, the nature of protagonists has evolved from the early emphasis on single white males in the mold of James Bond. *Enter the Dragon* (1973) features an Asian main character, played by Bruce Lee, who spies on a drug cartel while taking part in a martial arts competition. Numerous “blaxploitation” movies of the 1970s feature African American law enforcement or intelligence operatives who usually uncover white perfidy and black collusion. By 2002, *Undercover Brother* spoofed these themes with its portrayal of an all-black intelligence organization called The Brotherhood, which is pitted against white enemies that include White She-Devil and The Man, both of them affiliated with the evil Operation Whitewash.

In *Undercover Blues* (1993), the spy team consists of a married couple (Dennis Quaid and Kathleen Turner) with a six-month-old baby. By then, women protagonists in espionage films were far from unusual. The mid-1980s featured a number of such films with female protagonists, examples being *The Little Drummer Girl* (adapted from a Le Carre novel, 1984), *Jumpin’ Jack Flash* (1986), and *Outrageous Fortune* (1987). All of these—starring Diane Keaton, Whoopi Goldberg, and Shelley Long respectively—played on the theme, made famous by Hitchcock, of the innocent caught up in clandestine activities. *Confessions of a Dangerous Mind* (2002) took this “innocent” theme a step further, with its tale of *Gong Show* host Chuck Barris’s alleged recruitment by U.S. intelligence.

*Drummer Girl* and *Jackal* (from a book by Frederick Forsythe) were just two of many book adaptations from the late twentieth and early twenty-first centuries. Particularly notable in this regard were adaptations of Tom Clancy’s Jack Ryan books, with Alec Baldwin playing Ryan in *The Hunt for Red October* (1990); Harrison Ford in *Patriot Games* (1992) and *Clear and Present Danger* (1994); and Ben Affleck in *The Sum of All Fears* (2002). Two books published much earlier, *Mother Night* by Kurt Vonnegut and *The Bourne Identity* by Robert Ludlum, were finally adapted for the screen in 1996 and 2002 respectively.

**Terrorism.** *Patriot Games* was just one of many films about terrorism, and terrorism in Northern Ireland particularly.

The trend began in the 1970s, as terrorism became an increasingly common element of modern life. *Black Sunday* (1977) portrayed fictional events, but many more have, either through drama or documentary, depicted real ones. Examples include *21 Hours at Munich* (1976), *Hijacking of the Achille Lauro* (1989) and *Voyage of Terror: The Achille Lauro Affair* (1990), and *The Tragedy of Flight 103: The Inside Story* (1990). The first World Trade Center bombing was the subject of *Without Warning: Terror in the Towers* (1993), while several documentaries, including *9–11: American Reflections* (2001), *9/11* (2002), and *WTC: The First 24 Hours* (2002), have portrayed the second attack.

Films on the Northern Ireland theme include *Harry’s Game* (1982), *The Crying Game* (1992), *In the Name of the Father* (1993), *Michael Collins* (1996), *The Boxer* (1997), *The Devil’s Own* (1997), and *The Jackal* (1997), a critically panned remake of *Day of the Jackal* with a change of scenery and characters. Depictions of terrorist-controlled hostage scenarios became popular after the success of *Die Hard* (1988). Many of these have featured airplanes, examples being *Die Hard 2* (1990), *Passenger 57* (1992), *Executive Decision* (1996), and *Air Force One* (1997). The plot of *Barcelona* (1994) includes terrorism of the Cold War era, while *Brazil* (1985) presents a vision of terrorism in the future. After the real-life events of September 2001, the theme has proven less popular in films. As a result of the bombings, Warner Brothers delayed release of its terrorist-related *Collateral Damage* (2002), which starred Schwarzenegger.

## ■ FURTHER READING:

### BOOKS:

- Birdwell, Michael E. *Celluloid Soldiers: The Warner Bros. Campaign Against Nazism*. New York: New York University Press, 1999.
- Gregg, Robert. *International Relations on Film*. Boulder, CO: Lynne Rienner Publishers, 1998.
- Lisanti, Tom, and Louis Paul. *Film Fatales: Women in Espionage Films and Television, 1962–1973*. Jefferson, NC: McFarland, 2002.
- Mavis, Paul. *The Espionage Filmography: United States Releases, 1898 Through 1999*. Jefferson, NC: McFarland, 2001.

### ELECTRONIC:

Internet Movie Database. <<http://us.imdb.com>> (April 30, 2003).

### SEE ALSO

*Assassination Weapons, Mechanical Black Ops Cameras, Miniature Drop Intelligence Literature Nuclear Regulatory Commission (NRC), United States*

## Mujahedin-e Khalq Organization (MEK or MKO)

The Mujahedin-e Khalq Organization (MEK or MKO) philosophy mixes Marxism and Islam. Formed in the 1960s, the organization was expelled from Iran after the Islamic Revolution in 1979. Prior to Operation Iraqi Freedom in March 2003, its primary support came from the Iraqi regime of Saddam Hussein. MEK history is studded with anti-Western attacks as well as terrorist attacks on the interests of the clerical regime in Iran and abroad. The MEK now advocates a secular Iranian regime.

The MEK also operates as, or is known as: The National Liberation Army of Iran (NLA, the militant wing of the MEK), the People's Mujahidin of Iran (PMOI), National Council of Resistance (NCR), Muslim Iranian Student's Society (front organization used to garner financial support).

**Organization activities.** The MEK worldwide campaign against the Iranian government stresses propaganda and occasionally uses terrorist violence. During the 1970s the MEK killed several U.S. military personnel and U.S. civilians working on defense projects in Tehran. It supported the takeover in 1979 of the U.S. Embassy in Tehran. In 1981 the MEK planted bombs in the head office of the Islamic Republic Party and the Premier's office, killing some 70 high-ranking Iranian officials, including Chief Justice Ayatollah Mohammad Beheshti, President Mohammad-Ali Rajaei, and Premier Mohammad-Javad Bahonar. In 1991, it assisted the government of Iraq in suppressing the Shia and Kurdish uprisings in northern and southern Iraq. Until Operation Iraqi Freedom the MEK continued to perform internal security services for Saddam Hussein's government. In April 1992, MEK conducted attacks on Iranian embassies in 13 different countries, demonstrating the group's ability to mount large-scale operations overseas. In recent years the MEK has targeted key military officers and assassinated the deputy chief of the Armed Forces General Staff in April 1999. In April 2000, the MEK attempted to assassinate the commander of the Nasr Headquarters—then the interagency board responsible for coordinating policies on Iraq.

The normal pace of MEK anti-Iranian operations increased during Operation Great Bahman in February 2000, when the group launched a dozen attacks against Iran. In 2000 and 2001, the MEK was involved regularly in mortar attacks and hit-and-run raids on Iranian military and law enforcement units and government buildings near the Iran-Iraq border. Since the end of the Iran-Iraq War the tactics along the border have garnered few military gains and have become commonplace. Prior to Operation Iraqi Freedom, MEK insurgent activities in Tehran constituted the biggest security concern for the Iranian leadership. In

February 2000, for example, the MEK attacked the leadership complex in Tehran that houses the offices of the supreme leader and president.

Prior to Operation Iraqi Freedom, several thousand MEK fighters were located on bases scattered throughout Iraq and armed with tanks, infantry fighting vehicles, and artillery. The MEK also had an overseas support structure. Most of the fighters were organized in the MEK's National Liberation Army (NLA). Following Operation Iraqi Freedom and the removal of Saddam Hussein's government in April 2003, the fate of the MEK remains undetermined.

In the 1980s the MEK's leaders were forced by Iranian security forces to flee to France. After resettling in Iraq in 1987, the group conducted internal security operations in support of Saddam Hussein's regime. In the mid-1980s the group did not mount terrorist operations in Iran at a level similar to its activities in the 1970s, but by the 1990s the MEK had claimed credit for an increasing number of operations in Iran. Beyond support from the former Iraqi regime, the MEK used front organizations to solicit contributions from expatriate Iranian communities.

### ■ FURTHER READING:

#### ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001. Annual Report: On the Record Briefing. May 21, 2002 <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

#### SEE ALSO

*Terrorism, Philosophical and Ideological Origins  
Terrorist and Para-State Organizations  
Terrorist Organization List, United States  
Terrorist Organizations, Freezing of Assets*

## Multisensory Grenades.

SEE *Audio Amplifiers.*

## Mustard Gas

### ■ JUDYTH SASSOON

Mustard gas is a substance used in chemical warfare. It is the popular name for the compound with the chemical



Blister on the legs of a Chinese soldier after exposure to mustard gas in 1941. ©BETTMANN/CORBIS.

designation 1,1-thiobis(2-chloroethane) (chemical formula:  $\text{Cl-CH}_2\text{-CH}_2\text{-S-CH}_2\text{-CH}_2\text{-Cl}$ ). Mustard gas has a number of other names by which it has been known over the years, including H, yprite, sulfur mustard and Kampstoff Lost. Because the impure substance is said to have an odor similar to that of mustard, garlic or horseradish, the name mustard gas is most commonly applied. However, in the pure form, mustard gas has neither color nor odor. The gas was used for the first time as an agent of chemical warfare during World War I, when it was distributed with devastating effect near Ypres in Flanders on July 12, 1917.

The synthesis of mustard gas was reported much earlier than its first use as a chemical weapon. In 1860, Frederick Guthrie observed that when ethylene reacted with chlorine a substance was produced which, in small quantities, could produce toxic effects on the skin. Exposure to low concentrations of mustard gas classically causes the reddening and blistering of skin and epithelial tissue. On inhalation, the gas will cause the lining of the lungs to blister and leads to chronic respiratory impairment. Higher concentrations of mustard gas will attack the corneas of the eyes and eventually cause blindness. Exposure to mustard gas can lead to a slow and painful death and any moist area of the body is especially susceptible to its effects. The compound is only slightly soluble in water, but it undergoes a hydrolysis reaction liberating highly

corrosive hydrochloric acid and several other vesicant intermediates, which are able to blister epithelial surfaces.

Despite the ease of hydrolysis, mustard gas may be preserved underground in a solid form for up to ten years. The reason for this is that in an environment where the concentration of water is relatively low, the reaction pathway proceeds to form an intermediate known as thiodiglycol. In a low moisture environment, most of the water available at the solid surface is used in this reaction. Subsequently, another intermediate in the reaction pathway, a sulfonium ion, reacts with the thiodiglycol in the place of water. This reaction then creates stable, non-reactive sulfonium salts, which can act as a protective layer around the bulk of the solid mustard preventing further degradation.

Mustard gas as a chemical weapon is a particularly deadly and debilitating poison and when it was first used in 1917, it could penetrate all the masks and protective materials that were available at that time. In more recent years, urethane was found to be resistant to mustard gas, and also has several other advantages for use in combat; urethane is tough, resistant to cuts and is stable at a wide range of temperatures.

Detoxification procedures from mustard gas are difficult because of its insolubility and also because of the drastic effects it can have on lung epithelial tissue following inhalation. During World War I, physicians had no curative means of treating the victims of mustard gas exposure. The only method of detoxification that was known involved a rather extreme oxidation procedure using superchlorinated bleaches, such as 5% sodium hypochlorite. Today, several novel methods of detoxification have been developed to counter the effects of mustard gas and these include the use of sulphuramine solutions and magnesium monoperoxyphthalate. The most effective method to date employs peroxy acids, because they are able to react quickly with the mustard gas. Furthermore, the addition of a catalyst can speed up the detoxification reaction even more effectively.

Although mustard gas has been shown to have long-term carcinogenic properties, it can also be used as an agent in the treatment of cancer. In 1919, it was observed that victims of mustard gas attack had a low white blood cell count and bone marrow aplasia (tissue growth failure). More detailed research in the years following 1946 showed that nitrogen mustards, which differ from traditional mustard gas, could reduce tumor growth in experimental mice by cross-linking DNA strands. It had been shown previously that the sensitivity of mouse bone marrow to mustard gas was similar to that of humans and more detailed research eventually led to successful clinical trials. Today, nitrogen mustards are part of the spectrum of substances used in modern anti-cancer chemotherapy. They are primarily used in the treatment of conditions such as Hodgkin's disease and cancers of the lymph glands.

■ FURTHER READING:

PERIODICALS:

Devereaux, A., D. E. Amundson, J. S. Parrish, and A. A. Lazarus. "Vesicants and nerve agents in chemical warfare: Decontamination and treatment strategies for a changed world." *Postgrad. Med.* 1 (2002): 90–96.

Evison, D., D. Hinsley, and P. Rice. "Chemical Weapons." *BMJ* 324 (2002): 332–335.

Jones, G. B. "From mustard gas to medicines: the history of modern cancer chemotherapy" *Chem. Herit.* 15 (1998): 8–9; 40–2.

ELECTRONIC:

United Kingdom National Archives Learning Curve. "Mustard gas." <<http://www.spartacus.schoolnet.co.uk/FWWmustard.htm>> (February 20, 2003).

SEE ALSO

*Nerve Gas*



## NAILS (National Automated Immigration Lookout System)

NAILS (National Automated Immigration Lookout System) is a centralized database and computing system used by entry inspectors to identify aliens not eligible for admission. NAILS (and the updated version, NAILS II) allows inspectors to quickly retrieve and review biographical or historical case data and was designed to facilitate evaluation of entrant status.

The primary source of data for the NAILS database is gleaned directly from data supplied by potential immigrants on entry and immigration documents. This base of data provides a framework for the addition of information obtained from other federal, state, and foreign agencies.

Following the September 11, 2001, terrorist attacks on the United States, the NAILS system drew criticism because it is essentially a name-based system that can be thwarted by the use of a false name or falsified supporting documents. By relying on names rather than biometrics, NAILS provided gaps through which determined terrorists could slip into the United States.

NAILS is a secure database with access restricted on a “need to know” basis that was, prior to March 2003, operated by the Immigration and Naturalization Service (INS). On March 1, the newly created United States Department of Homeland Security (DHS) absorbed the former Immigration and Naturalization Service (INS). All INS border patrol agents and investigators—along with agents from the U.S. Customs Service and Transportation Security Administration—were placed under the direction of the DHS Directorate of Border and Transportation Security (BTS). Responsibility for U.S. border security and the enforcement of immigration laws was transferred to BTS.

BTS is scheduled to incorporate the United States Customs Service (previously part of the Department of

Treasury), and the enforcement division of the Immigration and Naturalization Service (previously part of the Department of Justice). Former INS immigration service functions are scheduled to be placed under the direction of the DHS Bureau of Citizenship and Immigration Services. Under the reorganization the INS formally ceases to exist on the date the last of its functions are transferred.

Although the description of the technologies involved in the NAILS entry security program remain the same as when operated by the INS, in an effort to facilitate border security, BTS envisions higher levels of coordination between formerly separate agencies and databases. As of April 2003, the specific coordination and future of the NAILS program was uncertain with regard to name changes, program administration, and policy changes.

Although the NAILS system is limited as an isolated system, even prior to DHS integration, data contained in the NAILS system, along with data from the Consular Lookout and Support System (CLASS), and the Treasury Enforcement Communications System (TECS II), was available to inspectors through the Interagency Border Inspection System (IBIS) maintained by U.S. Customs Service.

One reason for separate database systems is that it allows easier compartmentalization of data, keeping classified information secure while allowing access to data that may be requested under the Freedom of Information Act (FOIA).

### ■ FURTHER READING:

#### ELECTRONIC:

Department of Homeland Security. April 2, 2003. <<http://www.dhs.gov/dhspublic/index.jsp>> (April 11, 2003).

Department of Homeland Security, Bureau of Citizenship and Immigration Services. Law Enforcement: The National Border Patrol Strategy. <<http://www.immigration.gov/graphics/publicaffairs/statements/igstate.htm>> (April 12, 2003).

## SEE ALSO

*APIS (Advance Passenger Information System)*  
*IBIS (Interagency Border Inspection System)*  
*IDENT (Automated Biometric Identification System)*  
*INSPASS (Immigration and Naturalization Service Passenger Accelerated Service System)*  
*PORTPASS (Port Passenger Accelerated Service System)*  
*SENTRI (Secure Electronic Network for Travelers' Rapid Inspection)*

## Name Recognition Software.

SEE *IBIS (Interagency Border Inspection System)*.

---

## Nanotechnology

---

■ K. LEE LERNER

Defense programs in many countries are now concentrating on nanotechnology research that will facilitate advances in such technology used to create secure but small messaging equipment, allow the development of smart weapons, improve stealth capabilities, aid in developing specialized sensors (including bio-inclusive sensors), help to create self-repairing military equipment, and improve the development and delivery mechanisms for medicines and vaccines.

Nanotechnology builds on advances in microelectronics during the last decades of the twentieth century. The miniaturization of electrical components greatly increased the utility and portability of computers, imaging equipment, microphones, and other electronics. Indeed, the production and wide use of such commonplace devices such as personal computers and cell phones was absolutely dependent on advances in microtechnology.

Despite these fundamental advances there remain real physical constraints (e.g., microchip design limitations) to further miniaturization based upon conventional engineering principles. Nanotechnologies intend to revolutionize components and manufacturing techniques to overcome these fundamental limitations. In addition, there are classes of biosensors and feedback control devices that require nanotechnology because—despite advances in microtechnology—present components remain too large or slow.

### Advances in Nanotechnology

Nanotechnology advances affect all branches of engineering and science that deal directly with device components

ranging in size between 1/10,000,000 (one ten millionth of a millimeter) and 1/10,000 millimeter. At these scales, even the most sophisticated microtechnology-based instrumentation is useless. Engineers anticipate that advances in nanotechnology will allow the direct manipulation of molecules in biological samples (e.g., proteins or nucleic acids) paving the way for the development of new materials that have a biological component or that can provide a biological interface.

In addition to new tools, nanotechnology programs advance practical understanding of quantum physics. The internalization of quantum concepts is a necessary component of nanotechnology research programs because the laws of classical physics (e.g., classical mechanics or generalized gas laws) do not always apply to the atomic and near-atomic level.

**Nanotechnology and quantum physics.** Quantum theory and mechanics describe the relationship between energy and matter on the atomic and subatomic scale. At the beginning of the twentieth century, German physicist Maxwell Planck (1858–1947) proposed that atoms absorb or emit electromagnetic radiation in bundles of energy termed quanta. This quantum concept seemed counter-intuitive to well-established Newtonian physics. Advancements associated with quantum mechanics (e.g., the uncertainty principle) also had profound implications with regard to the philosophical scientific arguments regarding the limitations of human knowledge.

Planck's quantum theory, which also asserted that the energy of light (a photon) was directly proportional to its frequency, proved a powerful concept that accounted for a wide range of physical phenomena. Planck's constant relates the energy of a photon with the frequency of light. Along with the constant for the speed of light, Planck's constant ( $h = 6.626 \times 10^{-34}$  Joule-second) is a fundamental constant of nature.

Prior to Planck's work, electromagnetic radiation (light) was thought to travel in waves with an infinite number of available frequencies and wavelengths. Planck's work focused on attempting to explain the limited spectrum of light emitted by hot objects. Danish physicist Niels Bohr (1885–1962) studied Planck's quantum theory of radiation and worked in England with physicists J. J. Thomson (1856–1940), and Ernest Rutherford (1871–1937) to improve their classical models of the atom by incorporating quantum theory. During this time, Bohr developed his model of atomic structure. According to the Bohr model, when an electron is excited by energy it jumps from its ground state to an excited state (i.e., a higher energy orbital). The excited atom can then emit energy only in certain (quantized) amounts as its electrons jump back to lower energy orbits located closer to the nucleus. This excess energy is emitted in quanta of electromagnetic radiation (photons of light) that have exactly the same



energy as the difference in energy between the orbits jumped by the electron.

The electron quantum leaps between orbits proposed by the Bohr model accounted for Planck's observations that atoms emit or absorb electromagnetic radiation in quanta. Bohr's model also explained many important properties of the photoelectric effect described by Albert Einstein (1879–1955). Einstein assumed that light was transmitted as a stream of particles termed photons. By extending the well-known wave properties of light to include a treatment of light as a stream of photons, Einstein was able to explain the photoelectric effect. Photoelectric properties are key to regulation of many microtechnology and proposed nanotechnology level systems.

Quantum mechanics ultimately replaced electron "orbitals" of earlier atomic models with allowable values for angular momentum (angular velocity multiplied by mass) and depicted electron positions in terms of probability "clouds" and regions.

In the 1920s, the concept of quantization and its application to physical phenomena was further advanced by more mathematically complex models based on the work of the French physicist Louis Victor de Broglie (1892–1987) and Austrian physicist Erwin Schrödinger (1887–1961) that depicted the particle and wave nature of electrons. De Broglie showed that the electron was not merely a particle but a waveform. This proposal led Schrödinger to publish his wave equation in 1926. Schrödinger's work described electrons as a "standing wave" surrounding the nucleus, and his system of quantum mechanics is called wave mechanics. German physicist Max Born (1882–1970) and English physicist P. A. M. Dirac (1902–1984) made further advances in defining the subatomic particles (principally the electron) as a wave rather than as a particle and in reconciling portions of quantum theory with relativity theory.

Working at about the same time, German physicist Werner Heisenberg (1901–1976) formulated the first complete and self-consistent theory of quantum mechanics. Matrix mathematics was well established by the 1920s, and Heisenberg applied this powerful tool to quantum mechanics. In 1926, Heisenberg put forward his uncertainty principle which states that two complementary properties of a system, such as position and momentum, can never both be known exactly. This proposition helped cement the dual nature of particles (e.g., light can be described as having both wave and particle characteristics). Electromagnetic radiation (one region of the spectrum that comprises visible light) is now understood to have both particle and wave like properties.

In 1925, Austrian-born physicist Wolfgang Pauli (1900–1958) published the Pauli exclusion principle states that no two electrons in an atom can simultaneously occupy the same quantum state (i.e., energy state). Pauli's specification of spin ( $+\frac{1}{2}$  or  $-\frac{1}{2}$ ) on an electron gave the two electrons in any suborbital differing quantum numbers (a system used to describe the quantum state) and

made completely understandable the structure of the periodic table in terms of electron configurations (i.e., the energy-related arrangement of electrons in energy shells and suborbitals).

In 1931, American chemist Linus Pauling published a paper that used quantum mechanics to explain how two electrons, from two different atoms, are shared to make a covalent bond between the two atoms. Pauling's work provided the connection needed in order to fully apply the new quantum theory to chemical reactions.

Advances in nanotechnology depend upon an understanding and application of these fundamental quantum principles. At the quantum level the smoothness of classical physics disappears and nanotechnologies are predicated on exploiting this quantum roughness.

## Applications

The development of devices that are small, light, self-contained, use little energy and that will replace larger microelectronic equipment is one of the first goals of the anticipated nanotechnology revolution. The second phase will be marked by the introduction of materials not feasible at larger than nanotechnology levels. Given the nature of quantum variance, scientists theorize that single molecule sensors can be developed and that sophisticated memory storage and neural-like networks can be achieved with a very small number of molecules.

Traditional engineering concepts undergo radical transformation at the atomic level. For example, nanotechnology motors may drive gears, the cogs of which are composed of the atoms attached to a carbon ring. Nanomotors may themselves be driven by oscillating magnetic fields or high precision oscillating lasers.

Perhaps the greatest promise for nanotechnology lies in potential biotechnology advances. Potential nano-level manipulation of DNA offers the opportunity to radically expand the horizons of genomic medicine and immunology. Tissue-based biosensors may unobtrusively be able to monitor and regulate site-specific medicine delivery or regulate physiological processes. Nanosystems might serve as highly sensitive detectors of toxic substances or used by inspectors to detect traces of biological or chemical weapons.

In electronics and computer science, scientists assert that nanotechnologies will be the next major advance in computing and information processing science. Microelectronic devices rely on recognition and flips in electron gating (e.g. where differential states are ultimately represented by a series of binary numbers ["0" or "1"] that depict voltage states). In contrast, future quantum processing will utilize the identity of quantum states as set forth by quantum numbers. In quantum cryptography systems with the ability to decipher encrypted information will rely on precise knowledge of manipulations used to achieve various atomic states.

Nanoscale devices are constructed using a combination of fabrication steps. In the initial growth stage, layers of semiconductor materials are grown on a dimension limiting substrate. Layer composition can be altered to control electrical and/or optical characteristics. Techniques such as molecular beam epitaxy (MBE) and metallo-organic chemical vapor deposition (MOCVD) are capable of producing layers of a few atoms thickness. The developed pattern is then imposed on successive layers (the pattern transfer stage) to develop desired three dimensional structural characteristics.

## Nanotechnology Research

In the United States, expenditures on nanotechnology development tops \$500 million per year and is largely coordinated by the National Science Foundation and Department of Defense Advanced Research Projects Agency (DARPA) under the umbrella of the National Nanotechnology Initiative. Other institutions with dedicated funding for nanotechnology include the Department of Energy (DOE) and National Institutes of Health (NIH).

**Research interests.** Current research interests in nanotechnology include programs to develop and exploit nanotubes for their ability to provide extremely strong bonds. Nanotubes can be flexed and woven into fibers for use in ultrastrong—but also ultralight—bulletproof vests. Nanotubes are also excellent conductors that can be used to develop precise electronic circuitry.

Other interests include the development of nanotechnology-based sensors that allow smarter autonomous weapons capable of a greater range of adaptations en route to a target; materials that offer stealth characteristics across a broader span of the electromagnetic spectrum; self-repairing structures; and nanotechnology-based weapons to disrupt—but not destroy—electrical system infrastructure.

### ■ FURTHER READING:

#### BOOKS:

Mulhall, Douglas. *Our Molecular Future: How Nanotechnology, Robotics, Genetics, and Artificial Intelligence Will Change Our World*. Amherst, NY: Prometheus Books, 2002.

#### PERIODICALS:

Bennewitz, R., et. al., "Atomic scale memory at a silicon surface." *Nanotechnology* 13 (2000): 499–502.

#### ELECTRONIC:

National Science and Technology Council. "National Nanotechnology Initiative." <<http://www.nano.gov/start.htm>> (March 19, 2003).

### SEE ALSO

DARPA (*Defense Advanced Research Projects Agency*)

## Napoleonic Wars, Espionage During

■ ALEXANDR IOFFE

The Napoleonic wars pitted France, led by Napoleon Bonaparte, against a number of countries in Europe from 1797 through 1815. At different times during this period, Great Britain, Austria, Russia, Prussia, Denmark, Sweden, and the Neapolitan Kingdom all waged war against France in various coalitions. The main rivals in this struggle were Great Britain and France. During this time, the methods of intelligence gathering, espionage, and counterespionage did not differ so much from modern methods, apart from the differences in technological progress. Compared to other periods, however, espionage was a much more intense activity during the Napoleonic wars. This rise in espionage activity resulted mainly from revolutionary events in France and the following French emigration, which was in turn, used by Britain to achieve their own goals.

France had one unsurpassed master of intrigue in the famous person of Joseph Fouché, who spied rampantly on his social and professional contacts alike. Fouché remained as permanent minister of police during four consecutive regimes: directory, consulate, empire, and the restored monarchy.

During this period, Switzerland became a place of intensive intelligence activity by Britain, mostly against France. In 1794 the new charge d'affaire of Great Britain was the newly arrived William Wickham (1761–1840), for whom his diplomatic work in Bern was a cover. Wickham's main activity was to collect information about France and to lead various royalist organizations, which acted inside France as well as abroad. In particular, Wickham organized invasions of royalist armies into France, one of which was the Quiberon Bay invasion of 1795; the effort failed within one month. Both Wickham's agents and those of the royalist organizations actively participated for almost three years in different conspiracies against France, but in 1797, many of those involved were arrested. Wickham was forced to leave Switzerland in 1798, but the successive charge d'affaire continued the same activity.

British espionage against the Italian Army of France was also well organized. Here, the main figures were Count d'Antreg, one of the organizers of the royalist underground, and the British diplomat Francis Drake. D'Antreg

received information from the generals of the French army, such as key information about the Egyptian expedition of Bonaparte. D'Antreg was arrested in 1797 by the French in Venice and was scheduled for extradition to France, but was first granted an audience with Napoleon. After gaining Napoleon's favor, d'Antreg was released on his word of honor. He was then quickly aided in an escape to Switzerland.

British intelligence agents pursued Napoleon and his army during the Egypt expedition, and even attempted to organize the general's assassination. One well-known attempt was organized by one of the top officers of the British intelligence service. A fellow officer named Foure was married to one of Napoleon's mistresses; the plan called for Madame Foure to carry out the assassination during one of her dalliances with Napoleon. Foure eventually refused his mission, and the plan was not executed.

Another attempt to assassinate Napoleon was made on December 24, 1800. The First Consul Napoleon was required to be present at a performance in the Paris Grande Opera. When Napoleon's carriage rushed along Saint Nicolas Street, an explosion resounded. Napoleon did not suffer; his carriage was driving too quickly, but the power of the explosion was such that almost 50 people were killed or wounded and 46 neighboring houses were damaged. The source was a barrel of gunpowder laced with shrapnel that was hidden in a harnessed wagon at the roadside. At first, the Jacobins were accused of the attempt, and some were executed. But those who headed the investigation quickly determined that it was the work of royalists through whom was apparent "the hand of London."

Yet another attempt on Napoleon was undertaken by royalists (again supported from London) in 1803 to 1804, but it was stopped by Fouche's police. Fouche identified the plotters using his "Chouan's Geography," an elementary data base (card-index) compiled in his ministry containing detailed information about 1000 active royalists. The French word *chouan* is associated with royalty, or in this case, royalists.

Britain also actively collected all possible information about France during the Napoleonic period. For this purpose they used (in addition to traditional methods) various royalist organizations (in particular the "Correspondence," which mainly collected intelligence data). Smugglers, and fishers, and the inhabitants of Jersey Island were also actively recruited, especially during the continental blockade, for contact between Britain and the continent, as well as for espionage. One of these Jersey inhabitants, a British agent, was able to make 184 spying trips from Jersey to France before he was eventually captured by the French and executed in 1808.

Led by Fouche, the French used counterespionage and organized the assassinations of unwelcome persons, or at the least, discredited them. One example is the brilliantly executed operation directed against the British diplomat Francis Drake. The French agent Mehde de la

Touch was sent to London, where with great difficulty he was able to gain the confidence of top British authorities. De la Touch was able to persuade them that he represented a Jacobin committee that wanted to overthrow Napoleon. De la Touch was put in contact with Drake, at that time the ambassador in Munich, Bavaria, and using Drake, the phony committee was able to swindle large amounts of money from the British government. After a long period of such activity, the French published this information in the French press, Drake was discredited, and was forced to flee from Munich.

Napoleon himself was also actively interested in espionage. Among Napoleon's secret agents, the most successful was the Alsatian Charles Schulmeister, a trader from Strasbourg. Schulmeister brilliantly infiltrated the Austrian army, including its intelligence service, and by collecting vital information from and disseminating misinformation to the Austrian military commanders, ensured Napoleon's victory in Austria.

The year 1805 marked the beginning of Napoleon's war with Austria and Russia. Schulmeister was sent to Vienna with the mission to discern the character and plans of General Karl von Mack, commander of the Austrian Army on the Danube. Schulmeister gained the confidence of those in the aristocratic circles of Vienna and was soon introduced to General Mack. Schulmeister then persuaded Mack that he represented a royalist opposition, showing him secret data about the French army, given to him according to Napoleon's order, and false documents about his own Hungarian aristocratic origin. Soon Schulmeister was completely trusted by Mack and, incredibly, was designated chief of intelligence in General Mack's army. Schulmeister immediately informed Napoleon about Mack's plans, and Napoleon, in turn, ordered the printing of false newspapers and letters detailing the unrest in the French army. Mack swallowed the bait. He assumed that France was close to an uprising, and believed the information that Napoleon's troops were retreating from the front line on the Rhine River. He began to pursue the French. Most likely Mack was surprised when he collided with the "retreated" corps of French General Ney, and then discovered French troops at his flanks and back. The army of the gullible general was surrounded in Uhlm, and all that was left to do was to surrender. Napoleon then gained one of his most famous victories at the battle of Austerlitz, captured Vienna, and installed Schulmeister as its chief of police.

Napoleon soon required the further services of Schulmeister in Germany, where the operative set up an effective spy cluster that provided Napoleon, for a while, with valuable information from adversaries to the East. Schulmeister was awarded wealth for his efforts, but longed for the Legion of Honor, which Napoleon never bestowed, claiming, "gold is the only suitable reward for spies." After Napoleon's defeat at Waterloo and subsequent exile, Schulmeister was arrested, and bought his freedom with his fortune. Years later and nearly penniless,

Schulmeister sold tobacco at a stand in Strasbourg and regaled customers with stories of espionage during the Napoleonic wars.

#### ■ FURTHER READING:

##### BOOKS:

Dallas, Gregor. *The Final Act: The Roads to Waterloo*. New York: Henry Holt and Co., 2001.

Durant, Will, and Ariel Durant. *The Age of Napoleon*. New York: Simon and Schuster, 1975.

##### ELECTRONIC:

Sparrow, Elizabeth. *Secret Service: British Agents in France, 1792–1815*. Woodbridge, UK: Boydell Press, 1999.

Hollins, David. "The Hidden Hand: Espionage and Napoleon." *Osprey Military Journal* Issue 2.2, Osprey Publishing, <<http://www.ospreypublishing.com/content4.php/cid=71>> (December 30, 2002).

##### SEE ALSO

*France, Intelligence and Security*

## NASA (National Air and Space Administration)

#### ■ MORGAN SIMPSON

The Department of Defense (DOD) and the National Aeronautics and Space Administration (NASA) have to date elevated aerospace technologies to great heights. In a July 31, 1915, interview in *Collier's Weekly*, aviation pioneer Orville Wright (1871–1948) said, "The greatest use of the aeroplane [airplane] to date has been as a tremendously big factor of modern warfare." His statement could also be considered true today, along with the role played by commercial transportation in world's affairs. The victory of the United States in Operation Iraqi Freedom in 2003 illustrated the utilization of air and space to quickly quell an opponent's fighting ability. In this conflict, air and space utilization came in the form of direct air support, air to ground strategic targeting, Global Positioning System (GPS) targeting, and aerospace reconnaissance, both airplane and satellite. This utilization of air and space remains among the most powerful physical tools for ensuring national security.

NASA and DOD joint research has propelled the advances that make air and space important military assets. NASA's part in national security strategy is not as substantial as it was during NASA's first 35 years of existence (during the space race), but it still plays an important



In a joint research project, the Defense Advanced Research Projects Agency, NASA, and the U.S. Air Force used a Grumman X-29 with a forward-swept wing in fighter research during the 1980's and 1990's. ©MUSEUM OF FLIGHT/CORBIS.

role. As a national icon, NASA inspires nationalism in the American people, and its achievements are projected worldwide as an exhibit of America's scientific ability. A superpower nation with a space program was historically perceived as a potential threat to other nations, as seen with the United States reaction to the launching of the Soviet Union's *Sputnik* during the Cold War. The nation's response was the creation of a national civilian air and space agency called NASA.

NASA aeronautical research spurred numerous advances in aviation from which the military benefited; early studies regarding lifting bodies and fly-by-wire aircraft, which used NASA-developed electronics to control the inherently unstable aircraft, are two examples. Many of the aerospace research projects at the Dryden Flight Research Center (DFRC) in California are joint projects that advance aerospace engineering, science, and develop military hardware. Some of the research involves speed of sound (sonic and supersonic) studies, aeroelastic wing research, lifting body studies, unmanned vehicles, and other proprietary research.

Even though DOD and NASA have different space programs, they share numerous resources and have many joint contracts that support both the DOD program and the NASA program. These range from the simple support contracts for routine battery maintenance to expansive operations such as communications and spacecraft tracking. Both organizations share launch pads for expendable launch vehicles. Some of the expendable launch vehicles at the Kennedy Space Center (KSC) at Cape Canaveral, Florida, are the Titan, Atlas, and Delta rockets. Launch and

other facilities at KSC are resources shared by NASA, the Navy, and the Air Force.

NASA played a direct role in national security by providing the means to take heavy payloads into orbit. DOD has made its most direct use of NASA equipment in utilizing the Space Shuttle to bring up numerous DOD payloads. The contents of many of these payloads are classified information. There have been ten DOD dedicated shuttle launches. They are STS 51C, 51J, 27, 28, 33, 36, 38, 39, 44, and 53 (STS, which stands for Space Transportation System, also known as the Space Shuttle). Many of these missions remain secret even today, although some general knowledge about national security-based payloads has been disseminated and reported. In *The Space Shuttle Roles, Missions and Accomplishments* space historian David M. Harland stated that the shuttle delivered three new reconnaissance satellites in recent years. One satellite, called Lacrosse, provides all-weather vehicle-tracking capability. Another satellite included an advanced geostationary listening post. The third satellite is considered to house advanced imaging capabilities. It remains a secret as to what other DOD dedicated missions delivered to orbit or accomplished using the shuttle. Classified DOD missions continue to be carried out today, but mainly utilize the expendable launch vehicles. DOD and NASA both frequently have multiple minor payloads in addition to the major payload on a mission (both shuttle and expendable) to save costs. Some of these minor payloads are DOD sponsored payloads.

At one point, the vision of routine Space Shuttle launches was so powerful that the Air Force reluctantly agreed to phase out expendable launch vehicles. The Air Force's acceptance of the shuttle came with imposing requirements on the shuttle to launch heavy payloads of up to 60,000 pounds and to provide a cargo bay of 18 meters. The shuttle's payload mass weight has been downgraded to increase its margin of safety. The failure of the shuttle to run routinely, once a week, and the *Challenger* accident in 1986 motivated the DOD and NASA to change the DOD's main launching platform back to the expendable launch vehicles. Department of Defense then moved to utilizing new heavy lifting expendable launch vehicles to replace the shuttle's heavy lifting capacity. These new heavy-launch expendable launch vehicles can deliver almost 50,000 pounds to low Earth orbit.

Launch vehicles, including the Space Shuttle, utilize hardware that could be used for military applications such as the sophisticated guidance and navigations systems. The loss of the Space Shuttle *Columbia* in 2003 required personnel to retrieve instrumentation from the crash site to secure it to protect the secrecy of the technology.

The most well known NASA personnel are its astronauts. Astronauts have been used to carry out the DOD dedicated Space Shuttle missions. This required the astronauts to receive training on the secret payloads in order to properly execute the mission. The classified information given to the astronauts is usually kept to a minimum of

relevant required knowledge. The payloads are normally loaded into the launch vehicle at the latest possible opportunity in order to maintain security. Shuttle astronauts repaired one DOD satellite via EVA (Extra Vehicular Activity), spacewalk, when it failed to start. The majority of astronauts chosen for these missions have a military background, mostly for the flight experience. It is difficult to define to what extent NASA personnel have worked on DOD payloads because of the classified nature and the numerous joint research activities.

The Air Force has had astronaut-like programs, such as the Spaceflight Engineers and the Military-Man-In-Space program. Before the shuttle, spaceflight engineers were recruited to utilize the Gemini spacecraft to go to a planned Manned Orbiting Laboratory. The orbiting laboratory was cancelled with the introduction of automated cameras on satellites. Afterwards, spaceflight engineers were Air Force pilots who would train to be the specialist that would fly on the shuttle to oversee specific DOD payloads. In January, 1985, Gary Payton (a Spaceflight Engineer) flew on the first dedicated DOD shuttle mission, STS 51C, to supervise the deployment of a classified payload. The spaceflight engineers program was later disbanded. The Military-Man-In-Space program was designed to determine the potential for humans to be used for Earth observations. Human vision and intelligence was found to be a valuable asset as remote sensors, because of man's adept ability to distinguish subtle variations in hues more accurately than cameras and film. Remote sensing from space with accurate ground truth can greatly enhance the understanding of large natural systems like forests and ocean dynamics.

NASA's main role for national security is to inspire the youth of today that will populate aerospace professions in the future. This pool of technically minded persons will give the DOD a more intelligent and numerous base from which to recruit a future workforce. High-risk technologies have the potential to provide tremendous benefit for mankind. For aeronautics, NASA research divisions are positioned to study more technologies for their own benefit as well as that of the DOD, and the nation as a whole.

#### ■ FURTHER READING:

##### BOOKS:

Harland, David M. *The Space Shuttle Roles, Missions and Accomplishments*. New York: John Wiley & Sons Ltd, 1998.

##### ELECTRONIC:

Dryden Flight Research Center. "Flight Research Milestones." <<http://www.dfrc.nasa.gov/Dryden/mistone.html>> (May 6, 2003).

##### SEE ALSO

*Geospatial Imagery*

*Infrared Detection Devices*  
*Near Space Environment*  
*Satellites, Spy*  
*Strategic Defense Initiative and National Missile Defense*  
*USSTRATCOM (United States Strategic Command)*

---

## National Archives and Records Administration (NARA), United States

---

The National Archives and Records Administration (NARA) is an independent government agency that stores and provides public access to historical and significant documents related to the American government and its citizens.

Before NARA was created in the 1930s, government documents were stored randomly, with little thought to preservation. As a result, many important works were destroyed in fires or floods, or lost in the transfer from one storage facility to another. In fact, the Declaration of Independence, a crucial piece of American history, nearly disappeared on one of its journeys. In the mid-1920s, Congress recognized the need for a central facility to house important government documents, and authorized funds for a national archives building. On June 19, 1934, President Franklin D. Roosevelt signed the National Archives Act. R.D.W. Connor became the first official national archivist.

Based in Washington, D.C., NARA's now monumental collection recounts the history of America—and Americans. Housed within its collection are some of the most famous documents in American history, including the Declaration of Independence, the U.S. Constitution, the Bill of Rights, and the historic Nixon audiotapes. NARA's thirty-three facilities hold more than four billion pages of government documents, nearly 300,000 films, fourteen million photographs and posters, and five million maps. In addition, NARA hosts many permanent and temporary exhibits showcasing historical documents, artwork, letters, and photographs, and holds the personal collections of every president from Herbert Hoover to George Bush. Everything within the collection is open to the American public.

Not only does NARA store historically important materials, it cares for them as well. Archivists sift through piles of government documents each year to determine which items deserve a place in its stacks. Conservators work diligently to preserve each document, cleaning, repairing rips, and restoring damaged bindings. Retrieval staff respond to nearly 800,000 public requests for information each year.

Protection of archived national icons, such as the Declaration of Independence and the Constitution, has

been identified as a high priority in the national strategy to prevent terrorism, and falls under the responsibility of the Department of Homeland Security.

### ■ FURTHER READING:

#### BOOKS:

Rudy Smith, Christina. *The National Archives and Records Administration (Know your Government)*. Philadelphia, PA: Chelsea House Publishers, 1989.

United States National Archives and Records Administration. *The National Archives in the Nation's Capital: Information for Researchers*. Washington, D.C.: National Archives and Records Administration, 2001.

#### ELECTRONIC:

U.S. National Archives & Records Administration. <<http://www.archives.gov/>>.

#### SEE ALSO

*FOIA (Freedom of Information Act)*  
*Libraries and Information Science (NCLIS), United States National Commission*

---

## National Command Authority

---

The national command authorities of a nation are the persons or officeholders (or their duly deputized alternates or successors) who have the legal power to direct military activities. In almost all national governments, ultimate national command authority rests in a single office or individual, but there are almost always others involved in carrying out military policy. In the United States, the national command authorities are the president, the secretary of defense, and/or their duly deputized alternates or successors.

One of the hallmarks of the American system, and that of virtually all constitutional democracies, is civilian control over the military. Therefore, ultimate military authority rests in the civilian chain of command, the national command authority. Highest in the chain of command, of course, is the president. However, the chief executive oversees so many aspects of national policy that even in wartime, his duties necessarily force his attention to be directed toward other matters. Therefore, the secretary of defense plays a critical role in the oversight of military action. He or she answers to the president, and in turn guides military action along two lines of authority.

On the one hand are military forces not specifically assigned to combatant commands. These answer to the chiefs of the services, who report to the secretaries of the military departments (Army, Navy, and Air Force). The secretaries are in turn subordinate to the secretary of

defense. On the other hand, there are combatant commands, whose commanders answer directly to the secretary of defense. During the Persian Gulf War of 1991, the distinction between these two lines of authority became particularly noticeable in the form of the war's two most prominent military figures: General H. Norman Schwarzkopf, commander of allied forces on the ground, and General Colin Powell, chairman of the Joint Chiefs of Staff.

#### ■ FURTHER READING :

##### BOOKS:

Gilmour, Robert S., and Alexis A. Halley. *Who Makes Public Policy? The Struggle for Control Between Congress and the Executive*. Chatham, NJ: Chatham House Publishers, 1994.

Richelson, Jeffrey T. *The U.S. Intelligence Community*, 4th ed. Boulder, CO: Westview Press, 1999.

Trask, Roger R., and Alfred Goldberg. *The Department of Defense, 1947–1997: Organization and Leaders*. Washington, D.C.: U.S. Government Printing Office, 1997.

##### SEE ALSO

*DoD (United States Department of Defense)*  
*Joint Chiefs of Staff, United States*  
*Persian Gulf War*

---

## National Drug Threat Assessment

---

The National Drug Threat Assessment (NDTA) is an annual report of the National Drug Intelligence Center that assists in the formation of United States counterdrug policy and strategy by identifying criminal trends. Created by the General Counterdrug Intelligence Plan of 2000, the NDTA gathers intelligence from national, state, and local agencies and indicators to determine the level of danger that marijuana, cocaine, heroin, and methamphetamines pose to American society.

The NDTA obtains information by collecting the National Drug Threat Survey from 2,600 participating local and state law enforcement groups. The national agencies that share information with the NDTA are: Drug Enforcement Administration; Federal Bureau of Investigation; U.S. Coast Guard; U.S. Customs Service; El Paso Intelligence Center; Financial Crimes Enforcement Network; Crime and Narcotics Center; National Institute on Drug Abuse; Substance Abuse and Mental Health Services Administration; and National Institute of Justice. The indicators used by the NDTA are: Arrestee Drug Abuse Monitoring Program, Drug Abuse Warning Network, Monitoring the Future Study, National Household Survey on Drug

Abuse, Parents' Resource Institute on Drug Education Survey, and Treatment Episode Data Set.

While overall demand for illegal drugs has remained stable, NDTA intelligence suggests changing patterns of consumption and trafficking. The increased production of high potency marijuana may lead to greater demand, while the use of methamphetamines is growing. Young adults who are part of the rave culture are taking a combination of MDMA and heroin as well as compound MDMA/methamphetamine tablets. They are increasingly obtaining these drugs from localized groups and individuals, as opposed to the Mexican and Colombian organizations traditionally associated with trafficking. This changing distribution pattern has led to the rising availability of these drugs in suburban and rural areas.

Law enforcement agencies must correctly allocate limited resources to effectively combat illegal drugs. The NDTA will likely remain in production as part of this war on drugs.

#### ■ FURTHER READING :

##### BOOKS:

National Drug Intelligence Center, United States Department of Justice. *National Drug Threat Assessment 2001: The Domestic Perspective*. Johnstown, PA: National Drug Intelligence Center, October 2000.

##### ELECTRONIC:

United States Department of Justice. "National Drug Threat Assessment 2002." December 2001 <<http://www.usdoj.gov/ndic/pubs/716/>> (March 11, 2003).

##### SEE ALSO

*Crime Prevention, Intelligence Agencies*  
*DEA (Drug Enforcement Administration)*  
*FBI (United States Federal Bureau of Investigation)*  
*Intelligence and Law Enforcement Agencies*  
*NDIC (Department of Justice National Drug Intelligence Center)*  
*NIJ (National Institute of Justice)*

---

## National Information Infrastructure Protection Act, United States

---

The national information infrastructure is the collective computer and communication system that facilitates the operation of banks, businesses, schools, media, and the government. This infrastructure is crucial to the national economy and has expanded rapidly during the last decade. Because the network is computer based in the transmission of data, however, it is also vulnerable. In 1995,

Congress passed the National Information Infrastructure Protection Act, a bill providing for increased security of federal and private computers, and Internet server systems.

The National Information Infrastructure Protection Act was created to further expand the protections granted by the Computer Fraud and Abuse Act of 1986. Under the new act, protective measures were extended to computer systems used in foreign and interstate commerce and communication. The bill consolidated several older laws, including standing espionage laws, and labeled new crimes for stealing classified information from government computers.

Privacy was another major concern expressed in the act. It further criminalized the use of government computers to obtain confidential records, such as individual tax or medical records. Violators would be subject to prosecution under federal law, and charged with a separate crime for the use of the computer to hack and disperse sensitive documents. If these documents were obtained and dispersed for personal gain or profit, the crime becomes a felony. Convicted common security hackers were thus sentenced more leniently than those who prosecutors demonstrated acted with malicious intent. In its final provision, the act identified and criminalized the practice of computer blackmail, that is the ransoming of stolen information or the demand for access to an online account.

Not only did the bill cover computer fraud, but it also had implications for copyright law and corporate espionage. A copyright law amendment to the National Information Infrastructure Protection Act sought to grant jurisdiction over certain web contents to individual parties. The bill failed because it would have placed regulations on the Internet. The issue of ownership in cyberspace, however, remains an unclear legal question.

Since the passage of the act, computer crimes continued to rise in number, but not in severity. Incidences of viruses, stolen identities, and computer espionage peaked before the turn of the new millennium.

#### SEE ALSO

*Computer Fraud and Abuse Act of 1986*  
*Computer Hackers*  
*Computer Hardware Security*  
*Information Security (OIS), United States Office of Internet Surveillance*

---

## National Intelligence Estimate

---

■ JUDSON KNIGHT

National Intelligence Estimates (NIEs) are reports by the National Intelligence Council (NIC), drawing on estimative

views from across the intelligence community. The practice of creating NIEs developed in the late 1940s and early 1950s, as a response to previous intelligence failures.

## Background on NIEs

Despite the many advances in military and civilian intelligence that attended the successful completion of World War II and the creation of the Central Intelligence Agency (CIA) two years later, both CIA and military intelligence were taken completely by surprise when North Korean troops invaded South Korea in June 1950. In the months leading up to the invasion, intelligence personnel attached to General Douglas MacArthur's Tokyo headquarters regularly issued reports that downplayed the threat from North Korea and its Chinese allies, whose entrance into the ensuing war in late 1950 would greatly expand the scale of the conflict. Determined to create a framework and mechanism for the production of reliable intelligence estimates, General Walter Bedell Smith, when he became Director of Central Intelligence (DCI) in October 1950, instituted the concept of the NIE.

Today NIEs are the responsibility of the NIC, which serves the entire intelligence community and reports to DCI in his capacity as head of that community. It is the job of the NIC to bring together estimative views, not only from the CIA, but also from the Defense Intelligence Agency, the four military services, the National Security Agency, the Department of State Bureau of Intelligence and Research, and the intelligence units of the Federal Bureau of Investigation, the Department of Energy, and the Treasury Department. The directors of all of these organizations together constitute the National Foreign Intelligence Board, which reviews each NIE and must approve it before it is sent to the president and other national leaders.

Since 1950, numerous NIEs have been produced, and those that relate to matters that are now moot—for example, the conflicts of Cold War era—have been declassified. This has enabled at least some analysis of their accuracy. On the negative side, an NIE in 1962 maintained that Russian president Nikita Khrushchev would not put missiles in Cuba, a prediction proven inaccurate by the Cuban Missile Crisis in October of that year. Likewise, NIEs failed to predict the Yom Kippur War of 1973, or the fall of the Shah of Iran in 1978. Most infamously, in 1989, an NIE showed that Saddam Hussein's Iraq, exhausted by an eight-year war with Iran, would not instigate any significant military actions in the next three years—a prediction proven wrong by the Iraqi invasion of Kuwait in August 1990.

Yet, there were also numerous successes in the NIEs regarding the nation that most clearly threatened U.S. national security in the years from 1950 to 1990: the Soviet Union. As with much else about intelligence work, where NIEs are concerned, it is primarily the failures that attract attention. Successes, on the other hand, either remain



hidden entirely from view, or, where the success in question is an accurate estimate or prediction, hindsight makes the wisdom behind it seem self-evident. Yet, as NIC director Joseph S. Nye, Jr., showed in a 1994 piece for *Foreign Affairs*, analysis of declassified materials indicates that NIEs on Soviet capabilities and intentions were usually quite accurate. Furthermore, NIEs on the situation in Vietnam during the 1960s tended to be much more accurate than the prognoses of the White House or the Pentagon: whereas the nation's military and political leaders continued to believe until early 1968 that victory was inevitable, NIEs offered gloomy estimates on the chances of a U.S. military victory in Southeast Asia much earlier.

Nye also noted that NIEs have been faulted for overestimating Soviet military strength, but much of this occurred in the era before reconnaissance satellites, when U.S. intelligence had to rely much more on the Soviets' own, often exaggerated, claims as to their military capabilities. By the late 1960s and early 1970s, when America had satellites in the skies, it was in retreat globally, and NIEs of the time tended to *underestimate* Soviet power. As for the failure of the intelligence community to predict the fall of the Soviet Union—a failure that led Senator Daniel Patrick Moynihan (D-NY) to call for the abolition of the CIA—Nye observed that even Soviet President Mikhail Gorbachev failed to predict that his government would collapse as quickly as it did.

**Developments of the 1990s and later.** In an attempt to develop better NIEs, Nye reported in 1994, the NIC had “increased its emphasis on alternative scenarios rather than single-point predictions.” On the one hand, NIEs were less likely to predict a specific outcome, and instead tended to offer a variety of possible results contingent on other events—even ones that might be considered unlikely. On the other hand, national intelligence estimates eschewed what Nye described as “vague words like ‘possibly’ or ‘small but significant chance’” in favor of numerical percentages or odds for or against a particular event occurring.

The terrorist attacks of September 11, 2001, present an example of an event that would have seemed preposterous if someone had predicted it even a few days earlier. Yet, in the aftermath, one of the first questions Americans asked themselves was how their national intelligence and security apparatus had failed to see the attacks coming. Later, as President George W. Bush began to call for a war on Iraq as a sponsor of international terrorism, this claim was news to much of the public. Yet, the CIA had in its files such damning information as the fact that Saddam and Osama bin Laden had signed a non-aggression pact as far back as 1993; that al-Qaeda operatives had received training in Baghdad; and that Iraqi intelligence officers had met with bin Laden in Afghanistan and the Sudan.

According to a blistering analysis by Jim Hoagland in the *Washington Post* in October 2002, the reason that this information had not reached the general public was that it

simply was not fashionable among policy circles in the 1990s. Under the administration of President William J. Clinton, Hoagland maintained, “the need not to know very much about Iraq and terrorism was very strong.” Due to predictive failures in the NIEs, Bush had not been inclined to trust them, but the character of post-September 2001, NIEs reflected a new direction in national intelligence. The threats of North Korean missile attacks, and al-Qaeda computer hackers, both treated as remote possibilities before, were now being taken more seriously in NIEs. In 2002 and 2003, the brinkmanship of North Korean dictator Kim Jong Il, along with the sensitive data found on captured al-Qaeda computers, reinforced the advisability of this change.

#### ■ FURTHER READING:

##### PERIODICALS:

- Donnelly, John. “N. Korean Missile Has U.S. Range.” *Boston Globe*. (February 13, 2003): A1.
- Gellman, Barton. “Cyber-Attacks by al-Qaeda Feared.” *Washington Post*. (June 27, 2002): A1.
- Hoagland, Jim. “CIA’s New Old Iraq File.” *Washington Post*. (October 20, 2002): B7.
- “Let’s Have Straight Talk on Missile Defenses.” *Aviation Week & Space Technology* 145, no. 16 (October 14, 1996): 86.
- Nye, Joseph S., Jr. “Peering into the Future.” *Foreign Affairs* 73, no. 4 (July/August 1994): 82.
- Wall, Robert. “Review of NMD Fallout Underway.” *Aviation Week & Space Technology* 152, no. 19 (May 8, 2000): 31–32.
- Zelikow, Philip. “The Global Infectious Disease Threat and Its Implications for the United States.” *Foreign Affairs* 79, no. 4 (July/August 2000): 154–155.

##### ELECTRONIC:

- National Intelligence Council. <<http://www.cia.gov/nic/>> (March 17, 2003).

##### SEE ALSO

- DCI (Director of the Central Intelligence Agency)*  
*Intelligence Community*  
*NFIB (United States National Foreign Intelligence Board)*  
*NIC (National Intelligence Council)*  
*Nongovernmental Global Intelligence and Security*

---

## National Interagency Civil- Military Institute (NICI), United States

---

The National Interagency Civil-Military Institute (NICI) is an educational institute—funded by the Department of

Defense (DOD) through the National Guard Bureau—with the mission of improving the efficiency and effectiveness of joint civilian and military initiatives. To this end, it provides education to middle- and upper-level managers from the military, law enforcement agencies, emergency management and public safety organizations, and community groups. Founded in 1989 as the National Interagency Counterdrug Institute, its initial areas of focus involved border security and drug interdiction efforts, but it has expanded its course offerings since that time.

An incident along the Mexican border in October 1988 prompted the founding of NICI during the following year. While conducting a routine patrol for drug smugglers in the California desert, three National Guard soldiers and five deputy sheriffs in a UH-1 helicopter spotted a suspicious-looking parked vehicle with its lights off. As they descended to get a better look at the vehicle, they crashed into a power line, and all eight were killed. Ironically, the vehicle that had caught their attention belonged to the U.S. Border Patrol.

The tragic incident highlighted the need for greater coordination and cooperation among military and law enforcement, and in 1989, Dr. William Jefferds, former deputy adjutant general of the California National Guard, submitted a proposal to the National Guard Bureau for an institute to train individuals and agencies in joint operations. Congress approved the plan for NICI, established at Camp San Luis Obispo in California.

Among the programs NICI has added over the years are counterdrug demand reduction training, included in 1992 and expanded two years later. In 1994, NICI added a course in military support to civil authorities (MSCA), and in the following year held its first international MSCA course, attended by participants from several former Soviet republics. Following several terrorist attacks during the mid-1990s, NICI in 1997 developed antiterrorism courses, as well as blocks of instruction in community response to emergencies. It also conducts force protection level II training under the guidance of the U.S. Military Police School.

#### ■ FURTHER READING:

##### PERIODICALS:

Haskell, Bob. "A Plan Well-Executed." *Soldiers* 53, no. 5 (May 1998): 38.

"Tuition-Free, Counter-Drug Courses Offered." *National Guard* 54, no. 10 (October 2000): 10.

##### ELECTRONIC:

National Interagency Civil-Military Institute. <<http://www.nici.org/>> (March 30, 2003).

##### SEE ALSO

*DOD (United States Department of Defense) Homeland Security, United States Department*

*Law Enforcement Training Center (FLETC), United States Federal*

## National Liberation Army (ELN)—Colombia

The National Liberation Army (ELN) in Colombia is a Marxist insurgent group formed in 1965 by urban intellectuals inspired by Fidel Castro and Che Guevara. ELN began a dialogue with Colombian officials in 1999 following a campaign of mass kidnappings—each involving at least one U.S. citizen—to demonstrate its strength and continuing viability and force the Pastrana administration to negotiate. Peace talks between Bogota and the ELN started in 1999 and continued sporadically through 2001 until Bogota broke them off. Negotiations ultimately resumed in Havana, Cuba, by the end of 2001.

**Organization activities.** The ELN uses kidnapping, hijacking, bombing, extortion, and guerrilla war. ELN boasts a modest conventional military capability. ELN annually conducts hundreds of kidnappings for ransom, often targeting foreign employees of large corporations, especially in the petroleum industry. ELN attacks frequently target energy infrastructure and the group has inflicted major damage on pipelines and the electric distribution network.

ELN has an estimated 3,000 to 5,000 armed combatants and an unknown number of active supporters. The ELN is active mostly in rural and mountainous areas of north, northeast, and southwest Colombia, and Venezuela border regions. Cuba provides ELN fighters some medical care and offers political consultation to its leadership.

#### ■ FURTHER READING:

##### ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001, Annual Report: On the Record Briefing. May 21, 2002. <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual Reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

##### SEE ALSO

*Terrorism, Philosophical and Ideological Origins Terrorist and Para-State Organizations Terrorist Organization List, United States Terrorist Organizations, Freezing of Assets*

## National Military Joint Intelligence Center

The United States National Military Joint Intelligence Center (NMJIC), sometimes called the National Military Joint Intelligence Alert Center, is the nerve center for defense intelligence activities in support of joint military operations. Located physically and administratively close to the Joint Chiefs of Staff (JCS), NMJIC is also the fullest realization of the joint intelligence center (JIC) principle that developed in the last days of the Cold War.

### The Fleet Intelligence Center falls victim to changing views.

One of the most significant agencies absorbed into the then-new NMJIC during the early 1990s was the United States Navy Fleet Intelligence Center (FIC). With precedents dating back to the early days of World War II, the FIC operated on shore and provided United States fleets with intelligence support. Out of these wartime foundations emerged Fleet Intelligence Center Pacific (FICPAC) in 1955, FIC Europe (FICEUR) in 1960, and FIC Atlantic (FICLANT) in 1968.

The last two merged in 1974 to form FIC Europe-Atlantic (FICEURLANT). FICPAC played a critical role in providing intelligence to United States Navy and Marine forces in Vietnam. With more than 500 active-duty personnel by 1991, FICEURLANT was the largest of the FIC units. As it turned out, 1991 also marked the end of FIC, which fell victim to changing times. However, the army and air force counterparts—the Analysis and Control Element and the Air Intelligence Squadron respectively—managed to survive the change.

As for the causes of this change, this emerged in the 1980s, a period that saw the rise in popularity of the unified command principle among United States military circles. According to this principle, unified or area commanders in chief would direct all United States military operations in a given geographic area. For their intelligence needs, they relied on the JIC. The latter served as J-2, or joint intelligence, making it a “one-stop shop” for the intelligence needs of a given combatant command.

**The nerve center of joint intelligence.** At the national level, the function of J-2 is performed by the Defense Intelligence Agency (DIA), which oversees NMJIC. The latter in turn supports JCS, serving their needs, as well as those of unified commanders. NMJIC maintains a focus on global indications and warnings (I&W; intelligence that relates to time-sensitive information involving potential threats); operational intelligence (intelligence involved in military planning for a particular theatre or area of operations); national targeting support (prioritizing areas for possible action); production of reports; and database management.

Located alongside the National Military Command Center and the Defense Collection Coordination Center, NMJIC monitors worldwide political and military developments on a 24-hour basis, with an eye toward crises that may require United States intervention. Among the components of NMJIC are an alert center, warning and crisis analysts, targeting specialists, and a network of intelligence personnel, some of whom may deploy in support of war operations. In addition to DIA and those organizations, such as FIC, that have been subordinated to NMJIC, the center also includes representatives of the National Security Agency, Central Intelligence Agency, State Department, Defense Mapping Agency, and other United States military services.

### ■ FURTHER READING :

#### BOOKS:

Richelson, Jeffrey T. *The United States Intelligence Community*, 3rd ed. Boulder, CO: Westview Press, 1995.

#### ELECTRONIC:

Appendix A: Joint and Naval Intelligence Organizations That Support Naval Operations. Navy Warfare Development Command. <<http://www.nwdc.navy.mil/Library/Documents/NDPs/ndp2/ndp20007.htm>> (January 22, 2003).

#### SEE ALSO

*DIA (Defense Intelligence Agency)*  
*Joint Chiefs of Staff, United States*

## National Preparedness Strategy, United States

Events of the 1990s, particularly the first World Trade Center bombing in 1993 and the Oklahoma City attack two years later, revealed that the continental United States was far more vulnerable to terrorist attack than Americans had supposed. The federal government’s response to these and other situations had been on an *ad hoc* basis, resulting in the establishment of response capabilities under various Cabinet-level departments. The result, in many cases, was disorganization and duplication of services. By 1999, leaders had recognized the need for a national preparedness strategy, and three years later, the General Accounting Office (GAO) established, in broad outlines, what such a strategy should entail.

**The 1999 study: a searing critique.** According to the results of a 1999 national vulnerability study, “The country’s

seeming inability to develop and implement a clear, comprehensive, and truly integrated national preparedness strategy means that the government and citizens was still seen as possibly incapable of responding effectively to a serious terrorist attack.” The report came from an 18-member commission, chaired by Virginia governor James S. Gilmore III (R) and composed of retired military leaders, as well as figures from the medical, emergency planning, and intelligence communities.

Much of the commission’s 67-page report, delivered to President William J. Clinton on December 15, was a critique of the existing system for terrorism and emergency response. Much of the dissatisfaction noted in the study came from state and local officials, who found that federal plans failed to take appropriate account of community needs. For example, much federal planning focused on the 220 largest cities in the nation, effectively leaving smaller communities to fend for themselves.

**The 2002 study: a guide to effective partnership.** Following the September 11, 2001, terrorist attacks, the administration of President George W. Bush commissioned the GAO to report on the needs and challenges associated with the formation of a cohesive national preparedness strategy. Patricia A. Dalton, strategic issues director for the GAO, delivered her report, *Combating Terrorism: Enhancing Partnerships through a National Preparedness Strategy*, on March 28, 2002.

As Dalton noted, the GAO had long called for a national terrorism preparedness strategy that would integrate federal, state, and local response capabilities. Such a strategy, according to GAO, should include definition and clarification of the roles and responsibilities of various entities; establishment of goals and performance measures; and thoughtful decision-making with regard to the tools that would best assist in implementing a national strategy.

An array of legislation and presidential directives addressed the national response to terrorism, including several bills introduced in Congress following the September 2001 attacks. Funding was in place, with \$29.3 billion allocated for homeland security in the 2002 budget and \$37.7 billion requested for 2003. What was most sorely lacking, Dalton’s report indicated, was an overall plan, and with some 40 government agencies devoted to dealing with terrorism, there was bound to be a great deal of redundancy, waste, and inefficiency.

Attempting to deal with these problems, Attorney General Janet Reno had in December, 1998, presented a five-year Interagency Counterterrorism Crime and Technology Plan, but GAO found it lacking in a system for measuring outcomes. Additionally, Reno’s plan failed to identify state and local government roles. “The emphasis,” Dalton noted, “Needs to be on a national rather than a purely federal plan.” Not only had local communities in many cases failed to receive adequate help from the

federal government due to a confusion of response capabilities, but even those parts of the federal government officially involved in some aspect of emergency response were sometimes left out of decision-making on relevant matters.

To improve the situation, Dalton recommended the establishment of a one-stop “clearinghouse” for federal assistance to state and local response organizations. In order to develop a comprehensive response capability, her report indicated, it would be necessary to streamline the emergency-response apparatus. Additionally, an effective national preparedness strategy would encourage much greater cooperation among federal agencies, and between agencies at the federal, state, and local levels.

#### ■ FURTHER READING :

##### BOOKS:

Dalton, Patricia A. *Combating Terrorism: Enhancing Partnerships through a National Preparedness Strategy*. Washington, D.C.: General Accounting Office, 2002.

##### PERIODICALS:

Melton, R. H. “Panel Criticizes U.S. Anti-Terrorism Preparedness.” *Washington Post*. (December 16, 1999): A6.

##### SEE ALSO

*GAO (General Accounting Office, United States) Radiological Emergency Response Plan, United States Federal United States, Counter-terrorism Policy World Trade Center, 1993 Terrorist Attack*

---

## National Response Team, United States

---

The United States National Response Team, an interagency group co-chaired by the Environmental Protection Agency (EPA) and the U.S. Coast Guard (USCG), is charged with emergency response planning and coordination. It does not respond directly to emergency situations, but rather supports incident response forces by distributing information, planning emergency responses in advance, and training personnel to deal with response. In addition to backing federal components of emergency response, it also supports regional response teams (RRTs).

NRT members, in addition to EPA and USCG, include the departments of Defense, Energy, Agriculture, Commerce, Health and Human Services, Interior, Justice, Labor, Transportation, and the Treasury; the Federal Emergency

Management Agency (FEMA); the General Services Administration; and the Nuclear Regulatory Commission. Each has a specific role to play, as coordinated by the NRT: USCG, for example—among its many responsibilities for the team—manages the National Response Center and maintains 46 round-the-clock staffed facilities in major U.S. ports. FEMA advises and assists lead agencies in coordinating relocation assistance.

Even those parts of the NRT whose functions are not normally associated with emergency response have significant roles to play. The Department of Agriculture, for instance, monitors the effect of hazardous substances on natural resources, as does the Department of Interior, through offices such as the Fish and Wildlife Service, Bureau of Mines, Geological Survey, and National Park Service. The Department of Labor conducts health and safety inspections at hazardous waste sites through its Occupational Safety and Health Administration.

Coordinating these efforts is the NRT itself, which ensures that the roles of each agency are clearly outlined in the National Contingency Plan. It supports the training, education, and preparedness of members, both through courses within and outside the NRT, and through member committees that include the Preparedness Committee, the Response Committee, and the Science and Technology Committee. In working with RRTs, the NRT reviews regional or area contingency plans, and monitors RRT effectiveness during an incident.

#### ■ FURTHER READING:

##### PERIODICALS:

"New Guidelines Offered for Emergency Response Plans." *Environmental Management Today* 7, no. 3 (July/August 1996): 5.

Soltis, Dan. "Integrated Emergency Response Plans Will Save U.S. Industry Millions." *Water Engineering & Management* 144, no. 2 (February 1997): 17.

Steinman, Adam H. "Streamline Your Facility's Emergency Response Plans." *Chemical Engineering* 106, no. 3 (March 1999): 102.

##### ELECTRONIC:

Emergency Response Program, National Response Team. Environmental Protection Agency. <<http://www.epa.gov/superfund/programs/er/nrs/nrsnrt.htm>> (March 30, 2003).

U.S. National Response Team. <<http://www.nrt.org/>> (March 30, 2003).

##### SEE ALSO

*Chemical Safety: Emergency Responses Coast Guard National Response Center Emergency Response Teams EPA (Environmental Protection Agency) FEMA (United States Federal Emergency Management Agency) Radiological Emergency Response Plan, United States Federal*

## National Security Act (1947)

■ ADRIENNE WILMOTH LERNER

In the aftermath of World War II, the United States government undertook a dramatic reorganization of the national military and intelligence community. Departments created for wartime operations, such as cryptology, intelligence, and domestic security, needed restructuring for useful peacetime employment. Congress, and a special council of presidential advisors, reviewed military and government operations. Based on their recommendations, the National Security Act of 1947 outlined the ambitious plan to unify the military departments under the direction of a cabinet-level secretary. The individual responsibilities of the army and navy were more clearly defined, and the air force was created. The National Security Act of 1947 created the National Security Council, a formal foreign policy and military advisory team for the president, and the Central Intelligence Agency (CIA). The act was amended several times between 1945 and 1985, yielding the current government, intelligence, and military structure present in the United States today.

Signed into law on July 26, the National Security Act of 1947 initiated an immediate reorganization of the intelligence community. During the war, the Office of Strategic Services (OSS) performed most intelligence operations and trained a new generation of intelligence personnel. Though the OSS was initially slated for dissolution after the war, advisors close to President Harry S. Truman convinced the president that the organization could be retooled for peacetime operation, especially as Cold War tensions with the Soviet Union mounted. The act thus established a civilian successor agency to the OSS, the Central Intelligence Agency (CIA). The CIA was granted a broader mission to collect foreign intelligence data and conduct strategic surveillance. The position of director of central intelligence was created to administer the new agency and serve as a liaison between the intelligence community and the executive branch. The act assigned the task of domestic intelligence to the Federal Bureau of Investigation (FBI).

To facilitate the sharing of information, the formation of strategic foreign policy, and the protection of national security, the National Security Act of 1947 established the National Security Council (NSC). Comprised of the president, vice president, secretary of state, and the secretary of defense, the council meets to discuss security, intelligence, and strategic issues. The director of central intelligence and the chairman of the Joint Chiefs of Staff serve on the NSC in an advisory capacity. The role of the council was intentionally left somewhat ambiguous in the act so that each president could use the council that best suited his administration and foreign policy agenda. The council mostly convened as an advisory board until the Nixon Administration when the NSC gained the permanence and prominence in foreign and strategic affairs that it has today.

The 1947 act substantially reordered the military, in addition to the intelligence community. The War Department was abolished, and its duties incorporated with those of the former Navy Department into the Department of Defense (DOD). The position of Secretary of Defense was created to govern the new Department of Defense, but the individual branches of military service retained their own Secretaries. The original National Security Act of 1947 has been amended several times to further alter the structure of the DOD. In 1949, the DOD was elevated to a high-level executive department and the secretary of defense gained more power over military department Secretaries. In 1986, the position of the secretary of defense was firmly established in the executive chain of command as part of revisions to national Continuity of Government plans.

The operational duties of the individual military branches were also altered by the adoption of the National Security Act. The organizational structure of the army remained the same, but new emphasis was placed on training and maintaining permanent, professional forces. The act granted the navy the ability to maintain airplane squadrons to conduct any flight operations that it deemed essential to its main sea operations. The navy also remained the governmental custodian of the marines. After the value of aircraft and air defenses were proved on the battlefields of Europe and in the Pacific Theater during World War II, the National Security Act of 1947 recognized the strategic need for a professional and permanent air fleet by creating the air force.

Amendments to the original 1947 act have changed some structural and functional aspects of the military and intelligence communities, but the basic structure remains in place today. The September 11 terrorist attacks on the United States sparked a reexamination of the structure of national intelligence services and the manner in which information is shared by government departments. The recent passage of the Homeland Security Act, and the creation of the Department of Homeland Security, signal the largest reorganization of government security and intelligence agencies since the National Security Act of 1947.

#### ■ FURTHER READING:

##### BOOKS:

Hogan, Michael H. *A Cross of Iron: Harry S. Truman and the Origins of the National Security State, 1945–1954*. Cambridge University Press, 1998.

U.S. Department of State. *Foreign Relations of the United States: Department of State, 1945–1950*. Washington, D.C., 1996.

##### SEE ALSO

*CIA (United States Central Intelligence Agency)*  
*CIA, Formation and History*  
*FBI (United States Federal Bureau of Investigation)*  
*National Security Advisor, United States*  
*NSC (National Security Council)*  
*NSC (National Security Council), History*

## National Security Advisor, United States

Officially known as the Assistant to the President for National Security Affairs, the National Security Advisor—the more commonly used title—has a role defined as much by the chief executive as by law. The position did not exist as such for more than a decade after the establishment of the National Security Council (NSC), nor does that legislation mention the role of the advisor. Yet, as the chief counsel to the president on matters of national security, the advisor holds a role of unquestioned significance.

**Beginnings of the NSC and the advisor's role.** The enabling legislation for the NSC, the National Security Act of 1947, created the body to serve as advisory board to the president on domestic, foreign, and military matters involving national security, and to facilitate cooperation between agencies on these issues. Intelligence and covert operations were not encompassed in that original mission, not so much because such matters are seldom mentioned in public law, but because at the time of that legislation—which also created the Central Intelligence Agency (CIA)—few guessed the importance these activities would gain in years to come.

The 1947 legislation created the NSC as a small permanent staff whose director would be an executive secretary appointed by the president. Nowhere was it stated that the president required to submit this appointment for Senate confirmation. In future years, this would keep the role of National Security Advisor independent from the inner politics, not only of the legislative branch, but also of the executive branch. Removed from Congress and the bureaucracy of the State and Department of Defense, the Advisor would be the president's own counsel.

Ironically, in 1947, these other centers of power each viewed the new council as advancing their own interests, but none could have guessed the changes that would take place. For example, a 1949 reorganization of the NSC reduced the influence of the Department of Defense by removing the three service secretaries (army, navy, air force) from its membership. And while President Dwight D. Eisenhower created the role of President's Special Assistant for National Security Affairs, the position had little of the significance the National Security Advisor took on under President John F. Kennedy.

**National Security Advisors.** Starting with President Eisenhower's Special Assistants, U.S. National Security Advisors have included:

- Robert Cutler (March 1953–April 1955)
- Dillon Anderson (April 1955–September 1956)
- Robert Cutler (January 1957–June 1958)



U.S. National Security Advisor Condoleezza Rice fields a question during a press briefing at the White House, November 1, 2001. ©REUTERS NEWMEDIA INC./CORBIS.

■ Gordon Gray (June 1958-January 1961)

Presidents Kennedy and Johnson:

- McGeorge Bundy (January 1961-February 1966)
- Walt W. Rostow (April 1966-December 1968)

Presidents Nixon and Ford:

- Henry A. Kissinger (December 1968-November 1975; served concurrently as Secretary of State from September 1973)
- Brent Scowcroft (November 1975-January 1977)

President Carter:

- Zbigniew Brzezinski (January 1977-January 1981)

President Reagan:

- Richard V. Allen (January 1981-January 1982)
- William P. Clark (January 1982-October 1983)
- Robert C. McFarlane (October 1983-December 1985)
- John M. Poindexter (December 1985-November 1986)
- Frank C. Carlucci (November 1986-November 1987)
- Colin Powell (November 1987-January 1989)

President George H. W. Bush:

- Brent Scowcroft (January 1989-January 1993)

President Clinton:

- W. Anthony Lake (January 1993-March 1997)
- Samuel R. Berger (March 1997-January 2001)

President George W. Bush:

- Condoleezza Rice (January 2001—)

The years from Kennedy onward have seen each president personalize his administration in part through his appointment of the National Security Advisor, and in smaller measures through aspects of the NSC itself. Bundy, under Kennedy and later Lyndon B. Johnson, was the first powerful National Security Advisor, but his influence appears minimal compared to that of the most powerful individual ever to hold the position: Henry Kissinger. Emblematic of Kissinger's role was the fact that for part of his tenure as National Security Advisor to presidents Richard M. Nixon and Gerald R. Ford, he also served as Secretary of State.

From the Nixon era onward, presidents have likewise placed their personal stamp on the NSC through presidential directives, classified orders often drafted with the assistance of the National Security Advisor. These orders became known, in turn, as National Security Decision Memorandums (Nixon and Ford), Presidential Directives (Carter), National Security Decision Directives (Ronald Reagan), National Security Directives (George H. W. Bush),

Presidential Decision Directives (William J. Clinton), and National Security Presidential Directives (George W. Bush).

#### ■ FURTHER READING :

##### BOOKS:

Best, Richard A. *The National Security Council: An Organizational Assessment*. Huntington, NY: Novinka Books, 2001.

Felix, Antonia. *Condi: The Condoleeza Rice Story*. New York: Newmarket Press, 2002.

Hillen, John. *Future Visions for U.S. Defense Policy: Four Alternatives Presented as Presidential Speeches*. New York: Council on Foreign Relations, 1998.

Kissinger, Henry. *Problems of National Strategy: A Book of Readings*. New York: Praeger, 1965.

Powell, Colin L., and Joseph E. Persico. *My American Journey*. New York: Ballantine Books, 1996.

##### ELECTRONIC:

Official Intelligence Documents. American Federation of Scientists. <<http://fas.org/irp/offdocs/>> (March 24, 2003).

##### SEE ALSO

*Executive Orders and Presidential Directives National Security Act (1947)*  
*NSC (National Security Council)*  
*NSC (National Security Council), History*  
*President of the United States (Executive Command and Control of Intelligence Agencies)*

---

## National Security Strategy, United States

---

The National Security Strategy (NSS), as its name suggests, is a document outlining the blueprint for national security envisioned by the president of the United States. It has been issued, on a more or less annual basis, by each administration since Congress mandated its issuance in 1986, but prior to the September 2002 NSS of George W. Bush, the strategy report was little more than a statement of existing policy. The 2002 NSS, however, was not merely the first statement of its kind by a new administration, it was the first statement of national security strategy in a new era.

### Early History of the NSS

From the time of President Richard M. Nixon in the early 1970s, it was routine for chief executives of the United States to issue statements of policy as it related to national

security. The issuance of these statements became law in 1986, when Congress passed the Goldwater-Nichols Act. This legislation, which represented the fourth major reorganization of the U.S. Department of Defense since World War II, mandated that the White House present Congress with an annual statement of national security policy.

The Goldwater-Nichols Act was an expression of longstanding congressional frustration with the executive branch when it came to making clear executive policy on national security. Congressional leaders never doubted that a consistent national security strategy existed, as U.S. Military Academy political scientist Don Snider observed in *Foreign Policy*, but by requiring the White House to make its policy explicit, Congress would have an opportunity to exert greater influence on that strategy. The Goldwater-Nichols Act would also have the effect of asserting greater civilian control over the military.

**NSSs under Reagan, Bush, and Clinton.** Congressional frustration with presidential administrations in the matter of national security strategy was a phenomenon that had little to do with political party lines. Even when the same party controlled both the Oval Office and Congress, as University of Virginia political scientist Larry Sabato noted in *Foreign Policy*, the relationship between the White House and Capitol Hill tended to be more competitive than cooperative. The history of the NSS has tended to reinforce, rather than overturn, that background of competition between the legislative and executive branches of the federal government.

The NSSs submitted by the administrations of presidents Ronald Reagan, George H. W. Bush, and William J. Clinton usually did little more than simply restate policies then in effect. They were often bland, inciting little discussion on Capitol Hill or elsewhere, and some seemed more like promotional brochures on administration policy than carefully reasoned documents of national security. In 1994, an angry Senator Strom Thurmond, one of those involved in passing the Goldwater-Nichols Act, complained that the reports “seldom met . . . expectations.”

Thurmond also noted that reports tended to be late, if presidents even bothered to submit them at all. For his first NSS, Clinton and his aides went through 21 drafts before finally submitting it, a year and a half after the due date. George W. Bush failed to submit his NSS on the due date, June 15, 2001, and in any case, events three months later would have rendered that NSS moot. As it was, Bush did not finally submit his first NSS until September 2002—and when he did, its tardiness was the least of its controversial aspects.

**The 2002 NSS.** Bush’s 2002 NSS was an extraordinary document in the fact that it provided the blueprint for the new era that began with the terrorist attacks of September 11, 2001, as well as a framework for U.S. action resulting



from those attacks. It is a detailed document outlining an aggressive, but idealistic foreign and military policy. At the time the 2002 NSS was published, it appeared that the United Nations (U.N.) would support Bush's plans to force Saddam Hussein of Iraq to comply with U.N. demands regarding disarmament—a support that evaporated when the moment of truth came—but in any case, Bush's NSS makes little mention of the U.N. or other international organizations. In fact, the preamble lists the U.N. along with other groups of much smaller stature, suggesting that the administration was already beginning to chart a course separate, if necessary, from the U.N.

The 2002 NSS recognizes that the United States carries unique responsibilities as the sole remaining dominant superpower and would guarantee peace, freedom, and prosperity to those who agreed to pursue those aims. In its pages, it outlines an eight-part strategy, in both general and specific terms, for defeating terrorism and tyranny, encouraging global trade as a means to prosperity, fostering freedom and respect for human life, helping to build democratic institutions and free societies, spurring economic and infrastructure development, building cooperation for peace with other nations, and reforming American national security institutions to meet those challenges.

#### ■ FURTHER READING:

##### PERIODICALS:

- Gaddis, John Lewis. "A Grand Strategy for Transformation." *Foreign Policy* no. 133 (November/December 2002): 50–57.
- Hirsch, Michael. "Bush and the World." *Foreign Affairs* 81, no. 5 (September/October 2002): 18–44.
- Lucia, Christine. "Counterproliferation at Core of New Security Strategy." *Arms Control Today* 32, no. 8 (October 2002): 30.
- Rice, Condoleezza. "Anticipatory Defense in the War on Terror." *New Perspectives Quarterly* 19, no. 4 (fall 2002): 5–8.

##### ELECTRONIC:

The National Security Strategy of the United States of America. <<http://www.whitehouse.gov/nsc/nss.html>> (March 18, 2003).

##### SEE ALSO

- Bush Administration (1989–1993), United States National Security Policy*
- Bush Administration (2001–), United States National Security Policy*
- Clinton Administration (1993–2001), United States National Security Policy*
- National Preparedness Strategy, United States NSC (National Security Council)*
- President of the United States (Executive Command and Control of Intelligence Agencies)*

*Reagan Administration (1981–1989), United States National Security Policy*

*September 11 Terrorist Attacks on the United States*

## National Security Telecommunications Advisory Committee

The National Security Telecommunications Advisory Committee (NSTAC) is a presidential advisory board composed of leaders in various key industries. Its membership is made up of thirty chief executives who represent the leading communications, network service, and information technology companies, as well as the most prominent firms in the areas of aerospace technology and finance. Created under Executive Order 12382, signed by President Ronald Reagan in September 1982, NSTAC has advised presidents on issues that include communications, information systems, protection of critical infrastructure, information assurance, and other concerns relating to national security and emergency preparedness (NS/EP).

A subsidiary of the National Communications System (NCS), NSTAC acts as a liaison between government agencies and the private sector. NCS is among the leading government agencies concerned with national security and emergency preparedness, and it works closely with NSTAC in assessing challenges to the communication infrastructure, as well as in implementing solutions. Among projects initiated by NSTAC is the National Coordination Center for Telecommunications (NCC), established in 1984, in which thirteen NSTAC member companies work with NCS to develop, protect, and update national security and emergency preparedness (NS/EP) facilities nationwide.

#### ■ FURTHER READING:

##### BOOKS:

*Fifteen Years of Serving the President, 1982–1997*. Washington, D.C.: National Security Telecommunications Advisory Committee, 1997.

##### ELECTRONIC:

National Security Telecommunications Advisory Committee. <<http://www.ncs.gov/NSTAC/nstac.htm>> (February 2, 2003).

##### SEE ALSO

*Communications System, United States National*

*Critical Infrastructure Assurance Office (CIAO), United States*

## National Telecommunications Information Administration, and Security for the Radio Frequency Spectrum, United States

The Federal Communications Commission (FCC) regulates airwaves in the United States, but in order to make necessary determinations regarding allocation, the FCC turns to the National Telecommunications Information Administration (NTIA). A unit of the Department of Commerce, NTIA works with a number of participants in the increasingly crowded radio spectrum, including the private sector, the Department of Defense (DOD), and various law enforcement and emergency response agencies. Its aim is to meet commercial needs for the radio spectrum while maintaining availability for defense and security communication.

Established in 1978 by Executive Order 12046, NTIA serves as the president's principal advisor on telecommunication policies. On behalf of the President, it manages the radio frequency spectrum, and, in conjunction with the FCC and Department of State, promotes U.S. interests regarding spectrum use at the international level. Among its most important work is management of that portion of the frequency spectrum below 3 GHz. Though this represents about 1 percent of the usable radio spectrum, more than 93 percent of all FCC licenses and federal government frequency authorizations lie within that range.

NTIA supports defense, law enforcement, and public safety in a number of ways. In the emergency conditions following the September 11, 2001, terrorist attacks, it responded by going into 24-hours-a-day, seven-days-a-week mode to process all requests for special frequency allocation, and fulfilled nearly 7,000 such requests from entities that ranged from DOD to the White House to the Red Cross. The relationship between NTIA and DOD is a particularly strong one, since 40 percent of all federal frequency allocations are for defense use. Some 56 percent of these are in support of land, sea, and air mobile operations by the military services. NTIA also works closely with the DOD Joint Spectrum Center.

During the late 1990s and early 2000s, NTIA found itself confronted with two examples of its classic challenge: meeting security needs on the one hand, and fostering commerce on the other. In the case of third-generation

(3G) mobile and satellite-based broadband, as well as that of ultra-wideband (UWB) technology, spectrum space was needed for new, highly significant telecommunications advances. In the case of the UWB allocation, critical government systems used some of the frequencies involved, so in 2000, the FCC began the process of attempting to integrate UWB devices without harming vital communications. To make this possible, NTIA conducted extensive measurements and analysis, including tests using the global positioning satellite (GPS) system.

### ■ FURTHER READING:

#### PERIODICALS:

"Commerce Secretary Participates in China/U.S. Telecom Summit." *Communications Today*. (October 6, 1997): 1.

Noguchi, Yuki. "'Star Trek' Tech Gets Limited Approval." *Washington Post*. (February 15, 2002): E1.

Stern, Christopher. "Federal Radio Spectrum up for Bid." *Broadcasting & Cable* 124, no. 7 (February 14, 1994): 46.

#### ELECTRONIC:

National Telecommunications and Information Administration. <<http://www.ntia.doc.gov/>> (March 28, 2003).

#### SEE ALSO

*Commerce Department Intelligence and Security Responsibilities, United States*  
*Electromagnetic Spectrum*  
*FCC (United States Federal Communications Commission)*  
*FM Transmitters*

## NATO (North Atlantic Treaty Organization)

### ■ CARYN E. NEUMANN

Headquartered in Brussels Belgium, the North Atlantic Treaty Organization (NATO) is a military and diplomatic alliance of countries in Europe and North America that offers security to its members by pooling military resources and sharing intelligence. Formed in 1949 during the initial years of the Cold War as a response to Soviet aggression, the first countries to join the alliance were Belgium, Canada, Denmark, Great Britain, Italy, Luxembourg, Netherlands, Norway, Portugal, United States, France, Spain, and Iceland. Greece and Turkey were added to NATO in 1952 while Germany was admitted in 1955 and Spain entered in 1982. With the collapse of the Soviet Union, former satellite states have begun to join NATO. The Czech Republic, Hungary, and Poland became members in 1999 while Bulgaria, Estonia, Latvia, Lithuania, Romania, Slovakia and Slovenia are expected to complete the membership process in 2004. The northern boundary



Thousands of ethnic Albanians waving Turkish and Albanian flags welcome Turkish NATO peacekeeping soldiers in Prizren, Yugoslavia, in 1999. AP/WIDE WORLD PHOTOS.

of the alliance is established at the North Pole, past the Northwest Territories of Canada, while the southern terminus is located at the Tropic of Cancer, which runs between Florida and Cuba.

The idea for NATO germinated as the Cold War descended. Some democratic nations of Europe feared that they had been so weakened by World War II that they did not have the strength to fend off an attack by an increasingly aggressive Soviet Union without American assistance. Policymakers hoped that future war could be avoided by declaring that an armed attack upon one NATO member constituted an attack upon all members and that the threat of U.S. involvement would act as a particularly powerful deterrent to the Soviets. The treaty establishing NATO was signed in Washington, D.C. on April 4, 1949, and then subsequently ratified by its member countries. The NATO signatories agreed that if such an armed attack occurred, each NATO member would assist the victimized state by taking individually and in concert with each other such actions deemed necessary, including the use of armed force, to restore and maintain international peace and security. The vagueness of the treaty meant that the exact mechanism of the alliance would develop over time. In the initial decade of its existence, NATO planned to deploy nuclear weapons in retaliation for a Soviet military

attack. Under influence from U.S. President John F. Kennedy, the doctrine of flexible response replaced massive retaliation and no longer would automatic use of nuclear weapons be NATO policy.

Although the United States has been the dominant member in the past, NATO is governed by a North Atlantic Council that consists of permanent representatives of all member countries, who meet weekly. The council explains NATO decisions to the general public and to non-member nations. It also bears responsibility for creating subsidiary bodies to foster the political work of NATO. The Supreme Allied Commander of the Supreme Headquarters Allied Powers Europe (SHAPE) handles the military responsibilities of NATO. This command is divided into three parts: Allied Forces North Europe (AFNORTH), Allied Forces South Europe (AFSOUTH), and Other Commands. AFNORTH protects Belgium, Czech Republic, Denmark, Germany, Great Britain, Luxembourg, Netherlands, Norway, Poland, North Sea, Irish Sea, English Channel, and the Baltic Sea. It consists of Allied Air Forces North based in Ramstein, Germany, and Allied Naval Forces North based in Northwood, United Kingdom. AFSOUTH covers Greece, Hungary, Italy, Spain, Turkey, Black Sea, Sea of Azov, the whole of the Mediterranean and the Atlantic approaches to the Strait of Gibraltar east of longitude 7°

23° 48' W, and an area around the Canary Islands and its associated airspace. Headquartered in Naples, Italy, the force is made up of Allied Air Forces South and Allied Naval Forces South. Other Commands included the Maritime Immediate Reaction Forces, which offers continuous naval protection, and the NATO Airborne Early Warning Force, which provides air surveillance.

The collapse of the Soviet Union has challenged NATO by removing its main reason for existence. The organization is struggling to find a new role and has begun to focus on the fight against terrorism. The NATO-Russia Council, established in 2002, is identifying opportunities for joint action in all areas of mutual interest but especially in the use of the military to combat terrorist attacks. The future will probably see increasing cooperation between these former enemies as NATO alters in response to changing transatlantic security needs.

#### ■ FURTHER READING :

##### BOOKS:

- Cook, Don. *Forging the Alliance: The Birth of the NATO Treaty and the Dramatic Transformation of U.S. Foreign Policy Between 1945 and 1950*. New York: Arbor House/William Morrow, 1989.
- Kay, Sean. *NATO and the Future of European Security*. Lanham, Maryland: Rowman and Littlefield, 1998.
- Park, William. *Defending the West: A History of NATO*. Brighton: Wheatsheaf, 1986.
- Schmidt, Gustav, ed. *A History of NATO: The First Fifty Years*. New York: Palgrave, 2001.

##### ELECTRONIC:

- NATO. "North Atlantic Treaty Organisation." January 31, 2003. <<http://www.nato.int/>> (February 1, 2003).
- NATO. "Supreme Headquarters Allied Powers Europe." January 31, 2003. <<http://www.nato.int/shape/index.htm>> (February 1, 2003).

##### SEE ALSO

- Cold War (1945–1950): The Start of the Atomic Age*
- Cold War (1950–1972)*
- Cold War (1972–1989): The Collapse of the Soviet Union*
- Kennedy Administration (1961–1963), United States National Security Policy*

---

## Natural Resources and National Security

---

#### ■ WILLIAM C. HANEBERG

The ability of a nation to grow and defend itself is controlled in large part by the availability of natural resources.

Nations that do not possess sufficient mineral, energy, agricultural, and water resources within their boundaries must obtain them on the international market, where prices can be volatile and supplies unreliable. In times of war, all or part of the international market may be inaccessible and critical resources unavailable for import.

Mineral and energy resources have become increasingly important since the advent of mechanized warfare. Even before that, however, other natural resources played an important role in the growth of nations. A seventeenth- or eighteenth-century ship of the line in the British Navy may have required 400,000 board feet of lumber, much of which came from Britain's colonies in North America. A typical suburban home in the United States, in comparison, might require about 2000 board feet of lumber. Timber and, in later years, coal and iron resources helped the British Empire to become a dominant world power in the seventeenth, eighteenth, and nineteenth centuries.

The word resource refers to a naturally occurring concentration of minerals or fuels, whereas the word reserve refers to the portion of a resource that meets minimum criteria related to its extraction and processing. An accumulation of gold, for example, may be a resource but not a reserve if it cannot be mined and refined using existing technology. Resources can become reserves over time as technology improves and the economics of extraction and processing change. Therefore, the distinction is one of economics and engineering rather than geology. Resources are described as being measured, indicated, or inferred depending on the degree of certainty with which they are known. A measured resource is one for which the size has been established by geologic mapping, test drilling, and sampling. An inferred resource is one for which there is a reasonable amount of geologic evidence, but that has not been verified by drilling or sampling. Reserves are similarly described as being proven, probable, or possible.

**Energy resources.** The ability of a modern nation to defend itself or, should it be aggressive, to expand its territory depends on a reliable source of energy. Until the beginning of the twentieth century, this meant coal. Although coal remains an important energy source that is used to generate most of the electricity used in the United States, it has been joined in strategic importance by petroleum and nuclear fuels. The United States currently imports more than 3 billion barrels of oil per year from countries ranging from neighboring Canada and Mexico to Saudi Arabia, Nigeria, Iraq, and Angola. Although the United States contains significant petroleum reserves, they are not large enough to satisfy the long-term demand. It is, in most cases, also more expensive to produce oil from domestic reservoirs than to import it from countries that have abundant and easily recovered petroleum resources. The federal government maintains a Strategic Petroleum Reserve to help offset the potential effects of an oil embargo or other supply interruption. President George W. Bush ordered the first ever emergency withdrawal from

the reserve in an attempt to stabilize world oil prices that were fluctuating in response to the 1991 Iraqi invasion of Kuwait.

Although the United States and Canada contain significant uranium reserves, the currently depressed price of uranium on the international market generally makes it less expensive to import this energy source than produce it domestically.

The worldwide distribution of energy resources such as coal, petroleum, and uranium ore is controlled by geology and is far from uniform. Some nations, therefore, have an abundance of resources whereas others have little or no domestic supply of strategically important materials. A lack of petroleum reserves forced Nazi Germany to embark on an ambitious synthetic fuels program during the 1930s. The raw material for the German synthetic fuel program was coal, of which Germany had abundant supplies and which had satisfied its industrial and military energy needs until the beginning of the 20th century. Two synthetic fuel processes were employed by the Germans. One process produced automobile and aviation fuel and the other produced lubricating oil and diesel fuel. Twenty-one synthetic fuel plants, some of them using forced labor, had been constructed in Germany by the end of World War II.

Other countries, most notably Persian Gulf states such as Saudi Arabia and Kuwait, have petroleum resources that are disproportionately rich in relation to their geographic size and, just as importantly, inexpensive to produce. Some of these countries have been able to form strategic alliances with larger nations that depend on their petroleum. In addition, cartels such as the Organization of Petroleum Exporting Countries (OPEC) can strongly influence prices by increasing or decreasing their production, as was proven by the 1973 oil embargo.

Another potentially important energy resource is hydroelectric power, which requires large rivers as well as the ability to construct technologically sophisticated dams and hydroelectric power plants. The production of both aluminum for aircraft and fissionable plutonium for weapons requires large amounts of electricity. Inexpensive and abundant hydroelectric power was therefore an important strategic asset to the United States during World War II. During that time, dams along the Columbia River provided electricity to aluminum smelters throughout the Columbia River Basin and Manhattan Project facilities at the Hanford Site in Washington.

**Mineral resources.** Mineral resources include the ores of base metals such as copper, iron, and lead as well as strategic and critical metals such as chromium, titanium, platinum, cobalt, manganese, indium, palladium, and others. The latter are metals that are used in nuclear reactors, jet aircraft engines, missiles, computers, and industrial machinery, but of which the United States has little or no domestic supply. Therefore, they must be imported from countries that include the former Soviet Union, Zaire, and

Zimbabwe. Guerrilla warfare in Zaire during the 1970s caused the worldwide price of cobalt to increase from \$6 to \$45 per pound, and a United Nations trade boycott of Rhodesia (now Zimbabwe) made it impossible to legally obtain chromium mined in that country.

The importance of critical and strategic metals to the security of modern nations was recognized by the United States during World War I, when tungsten, tin, chromite (chromium ore), optical grade glass, and manila fiber for ropes were all in short supply. The War Department subsequently prepared a list of 28 materials that had been in short supply during World War I, and since then Congress has funded stockpiles of strategic materials that are essential for national security. The United States Geological Survey began its strategic minerals program in 1939, first concentrating on seven strategic metals and then expanding the program to include base metals and petroleum. Even with strategic minerals programs in place and stockpiles established before the war, conservation and recycling were essential during World War II. After the war, the Defense Minerals Administration was formed in 1951 to promote mineral exploration and development in the interest of national security, and its successor agencies were eventually merged into the Geological Survey.

**Agricultural land and water.** A third class of natural resources that is vital for national security includes agricultural land and water. As is the case for other resources, food or water that cannot be produced within a nation must be imported. Therefore, countries with large amounts of arable land, favorable climates, and fresh water can be less dependent on outside supplies than nations that lack one or more of those resources. In cases where technological solutions do exist, for example desalinization of seawater to produce drinking water in arid coastal areas, they can be too expensive for all but the wealthiest of nations.

#### ■ FURTHER READING:

##### BOOKS:

- Deffeyes, K. S. *Hubbert's Peak: The Impending World Oil Shortage*. Princeton, New Jersey: Princeton University Press, 2001.
- Yergin, Daniel. *The Prize: The Epic Quest for Oil, Money, and Power*. New York: Simon and Schuster, 1991.
- Youngquist, W. L. *GeoDestinies*. Portland, Oregon: National Book Company, 1997.

##### ELECTRONIC:

- Cartwright, M. R. "Mineral Resources/Reserves in Appraisal." March 21, 1999. <[http://www.minval.com/reserve\\_mineral.html](http://www.minval.com/reserve_mineral.html)> (14 December 2002).
- Energy Information Administration. "Imports of Crude Oil into the United States by Country of Origin, 2001." June 18, 2002. <<http://www.eia.doe.gov/ncic/rankings/crudebycountry.htm>> (14 December 2002).

Energy Information Administration. "25th Anniversary of the 1973 Oil Embargo." March 7, 2000. <<http://www.eia.doe.gov/emeu/25opec/anniversary.html>> (14 December 2002).

Stranges, A. N. "Germany's Synthetic Fuel Industry 1927–45." October 26, 2000. <<http://www.caer.uky.edu/fseminar/fsstrang.htm>> (14 December 2002).

U.S. Department of Energy. "Profile of the Strategic Petroleum Reserve." <<http://www.fe.doe.gov/spr/>> (14 December 2002).

#### SEE ALSO

*Bush Administration (1989–1993), United States National Security Policy*

*DOE (United States Department of Energy)*

*Energy Technologies*

*Petroleum Reserves, Determination*

---

## Navy Criminal Investigative Service (NCIS)

---

The Navy Criminal Investigative Service (NCIS) is responsible for providing law enforcement on behalf of United States Navy and Marine Corps personnel and their families. Originally part of the Office of Naval Intelligence (ONI), the organization was staffed primarily by military personnel, whereas today it is a largely civilian organization. NCIS has been involved in murder investigations and drug sweeps, and since September 11, 2001, it has also taken on a homeland security role.

NCIS began as part of ONI, which was deployed during World War II to detect potential spies and saboteurs on the domestic front. Through the end of World War II, the investigative branch of ONI was composed mainly of military personnel. In the postwar era, however, the Secretary of the Navy developed a coterie of civilian agents responsible for conducting criminal investigations, counterintelligence, and security background investigations on naval and marine personnel and civilians associated with the U.S. Navy and Marine Corps.

Only on February 4, 1966, did the Naval Investigative Service (NIS), as NCIS's predecessor was called, gain an identity separate from that of ONI. Nonetheless, it remained a part of the naval intelligence office. In 1972, the newly formed Defense Investigative Service took over responsibility for background checks, leaving NIS free to concentrate on counterintelligence and criminal investigations. During the 1980s, the organization went through a number of name changes until, in December 1992, it gained its present identity.

At the time of its establishment as NCIS, a civilian director, Roy D. Nedrow (formerly with the U.S. Secret Service), assumed leadership. During the following year,

he undertook reorganization in accordance with the broader downscaling of military and security organizations that attended the end of the Cold War. Whereas in 1991, NCIS had 2,281 personnel, including 1,167 civilian special agents operating in more than 200 offices worldwide, a decade later its ranks numbered 1,603, of whom 877 were civilian special agents operating in some 150 offices worldwide. In addition, 51 military agents, most of them from the Marine Corps, were assigned to NCIS. As part of Nedrow's reorganization, NCIS was restructured as a federal law-enforcement agency with 14 field offices.

**NCIS at work.** NCIS has received numerous accolades for its efficiency, not least for the work of its "cold-case squad," which has reopened scores of previously unsolved homicide cases, and successfully solved dozens. Working with the cold-case squad of the Fairfax County, Virginia, law-enforcement authorities, for instance, NCIS helped solve a homicide case that was extremely "cold" (old)—so much so that the accused had finished high school, had a full career in the Navy, and retired—all in the quarter-century between the murder and his arrest.

The case involved Paul S. Sorensen, who was 16 years old in 1975, when he allegedly stabbed to death a convenience store clerk while robbing a 7-Eleven. Sorensen entered the Navy after graduating high school in 1976, and in 1999, having attained the rank of chief petty officer, retired to Corpus Christi, Texas. Three years later, and five years after NCIS and Fairfax County reopened the cold case, Sorensen—knowing that he would soon be arrested anyway—turned himself in to authorities.

Another example of NCIS at work was the drug sweep that in July 2002 netted 84 marines and sailors at Camp Lejeune, North Carolina. Code-named Operation Xterminator, the sweep took two years and yielded \$1.4 million in narcotics. NCIS has also been involved in homeland security since the September 2001 terrorist attacks on the United States. Not only has the agency helped provide security for the naval base at San Diego Bay in California, but NCIS agents have taken part in community education programs designed to teach civilians how to monitor their neighborhoods for suspicious activity.

#### ■ FURTHER READING:

##### BOOKS:

*The Naval Criminal Investigative Service: To Protect and Serve.* Washington, D.C.: U.S. Department of the Navy, 1994.

##### PERIODICALS:

Crawley, James W. "Details of Port Security Are Off-Limits." *San Diego Union-Tribune*. (August 23, 2002): B1.

"Drug Sweep Nets 84 Marines, Sailors." *Commercial Appeal* (Memphis, TN). (July 3, 2002): A4.

Jackman, Tom. "Retiree Surrenders in 1975 Va. Killing." *Washington Post*. (May 22, 2002): B7.

#### ELECTRONIC:

Naval Criminal Investigative Service. <<http://www.ncis.navy.mil>> (January 18, 2003).

#### SEE ALSO

*Military Police, United States*

---

## NCIX (National Counterintelligence Executive), United States Office of the

---

Formerly known as the National Counterintelligence Center (NACIC), the U.S. Office of the National Counterintelligence Executive (NCIX) was created early in the twenty-first century. It educates members of government organizations and the private sector on the need to maintain vigilance against espionage, both the political and national forum and in the economic and industrial arena. NCIX conducts regional seminars, issues publications, and produces other materials in support of its mission to provide the federal government with strong policy leadership in the area of counterintelligence education.

### Establishment of the NCIX

Just two weeks before leaving office, on January 5, 2001, President William J. Clinton issued Presidential Decision Directive (PDD) 75, "U.S. Counterintelligence Effectiveness—Counterintelligence for the Twenty-first Century." PDD 75 presented specific measures that would enhance the ability of members of the U.S. counterintelligence (CI) community to identify and counteract threats.

First among the provisions of PDD 75 was the establishment of the Counterintelligence Board of Directors, which would be chaired by the director of the Federal Bureau of Investigation (FBI) and composed of the Deputy Secretary of Defense, the Deputy Director of Central Intelligence, and a senior representative of the Department of Justice. The directive also established the position of CI executive, or NCIX, to undertake certain responsibilities on behalf of the Board.

The NCIX, who would serve as a *de facto* director of counterintelligence activities at the national level, would be a federal employee selected by the board with the agreement of the Attorney General, Director of Central Intelligence, and the Secretary of Defense. The NCIX would

work closely with the National Coordinator for Security, Infrastructure Protection, and Counterterrorism. He or she would report to the FBI director, as board chairperson, but would be accountable to all board members, and would have the responsibility of advising them on counterintelligence programs, policies, and challenges.

PDD 75 went on to stipulate that the NCIX would chair the National Counterintelligence Policy Board, whose members would include (at a minimum) senior counterintelligence officials from the departments of State, Defense, Justice, and Energy, as well as from the Joint Chiefs of Staff, Central Intelligence Agency, FBI, and National Security Council (NSC). The NCIX would also oversee the Office of the National Counterintelligence Executive, which would replace the old NACIC.

**NACIC background and the change to the Office of the NCIX.** Whereas the new Office of the NCIX was ultimately under the leadership of the FBI, the NACIC had been attached to the NSC. Established by an earlier Presidential Decision Directive, in 1994, NACIC was also responsible for guiding U.S. counterintelligence activities. It was controlled by a National Counterintelligence Policy Board directed by the NSC, and had a number of functions, among them efforts to counter economic or industrial espionage.

In this capacity, the NACIC operated a threat assessment office that compiled information—both from the U.S. Intelligence Community and from open sources in the media and elsewhere—on activities by foreign powers and their intelligence agencies that posed a potential threat to U.S. companies. NACIC also analyzed possible espionage concerning emerging technologies from the United States, as well as threats to U.S. executives or business personnel. It also kept a close watch on the effects of foreign ownership, technology transfers, and joint ownership on U.S. economic concerns.

As would be the case later with the Office of the NCIX, the NACIC made available to the U.S. business community its reports on economic espionage, and sought to strengthen ties between private enterprise and federal agencies for enhanced counterintelligence awareness. PDD 75 ensured that those activities would continue, but under the direction of the FBI. On November 27, 2002, Public Law 107-306 formally established the Office of the National Counterintelligence Executive.

**An expanded outreach to the private sector.** The new Office of the NCIX expanded the outreach to the private business community undertaken by the NACIC. The latter had already been conducting regional seminars on CI, but due to a lack of private-sector security organizations involved in administering the seminars, their visibility had been limited. The new office, instead of appealing to those few civilian security organizations (examples included the National Classification Management Society, as well as

various Industrial Security Advisory councils), sought to broaden its appeal.

The Office of the NCIX also created, and made available to the private sector, a vast array of products designed to enhance awareness of CI. The office published on the Internet its *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage*, as well as its *Counterintelligence News and Developments (CIND)* newsletter. It also published booklets and brochures such as *Be Alert!*, designed to instruct American travelers abroad as to the ways that they might become targets of foreign intelligence collection activities. At its Web site, the Office of the NCIX also sold videos such as *Insider Betrayal*, regarding FBI and private-sector cooperation to counter economic espionage. It also sold posters, and made available for free various computer screen savers and background screens designed to heighten awareness of counterintelligence.

#### ■ FURTHER READING:

##### BOOKS:

*Survey of the Counterintelligence Needs of Private Industry*. Washington, D.C.: National Counterintelligence Center, 1995.

##### PERIODICALS:

Barth, Steve. "Spy vs. Spy." *World Trade* 11, no. 8 (August 1998): 34–37.

Gottlieb, Daniel W. "Keeping Trade Secrets Secret: Counterspies, Codes Courts." *Purchasing* 126 no. 7 (May 6, 1999): 24–25.

Kaltenhauser, Skip. "Industrial Espionage Is Alive and Well." *World Trade* 10, no. 7 (July 1997): 24–26.

##### ELECTRONIC:

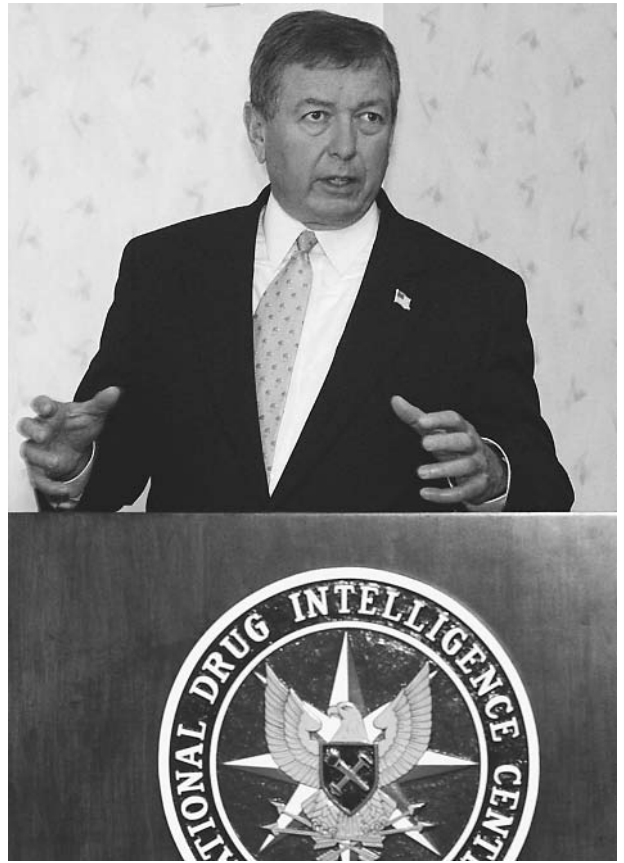
Office of the National Counterintelligence Executive. <<http://www.ncix.gov>> (March 17, 2003).

##### SEE ALSO

*Economic Espionage*  
*Economic Intelligence*  
*Intelligence Community*

## NDIC (Department of Justice National Drug Intelligence Center)

The Department of Justice National Drug Intelligence Center (NDIC) is the lead counterdrug agency within the U.S.



Attorney General John Ashcroft, speaking at a news conference at the National Drug Intelligence Center in Johnstown, Pennsylvania, in August, 2002, said that the technology now being used to combat illicit drugs has also proven useful in tracking the movement of terrorist groups. AP/WIDE WORLD PHOTOS.

intelligence community. Created in 1993, it is responsible for providing national leadership as well as law enforcement officials, with a strategic picture of the traffic in illegal drugs throughout the United States. It offers its client base a number of intelligence products and services, including information provided by its Document Exploitation Division.

**NDIC products and services.** Principal among NDIC's intelligence products are its threat assessments, of which the most significant is its annual National Drug Threat Assessment. The latter identifies principal drug threats, provides data on changes in consumption patterns, analyzes the availability of drugs by geographic market, and tracks patterns of distribution and trafficking. NDIC also creates drug threat assessments by state, and issues information bulletins in response to drug-related issues as those arise.

The Intelligence Division of NDIC includes six geographic units, as well as four units with specialized tasks. These are the Drug Trends, Organized Crime and Violence, National Drug Threat Assessment, and National Interdiction



Support units. Some information comes to NDIC by means of field program specialists, whose position was created by a January 2001 initiative intended to encourage sharing of information among law-enforcement officials at the federal, state, and local levels. Field representatives are independent contractors, usually with years of experience in drug law enforcement.

NDIC's Document Exploitation Division analyzes information seized in major federal drug raids or investigations. Document Exploitation teams make use of proprietary software known as the Real-time Analytical Intelligence Database, or RAID. RAID allows agents to process massive quantities of information from seized documents and computers. The program collects, collates, and labels large information packets, then subject this data to intensive analysis in a search for hidden information on assets, associates, and other valuable leads.

The center also provides counterdrug analysis training courses for personnel in local, state, and federal law enforcement agencies. This education program is a cooperative effort of NDIC and the Federal Bureau of Investigation, Drug Enforcement Administration, National Guard Bureau, U.S. Customs Service, and Financial Crimes Enforcement Network. In performing its overall mission, NDIC works closely with these agencies, as well as with the U.S. Coast Guard, the Bureau of Alcohol, Tobacco, and Firearms, the Bureau of Prisons, and the Office of National Drug Control Policy.

## ■ FURTHER READING:

### PERIODICALS:

Strong, Ronald L. "The National Drug Intelligence Center: Assessing the Drug Threat." *The Police Chief* 68, no. 5 (May 2001): 55–60.

### ELECTRONIC:

National Drug Intelligence Center. <<http://www.usdoj.gov/ndic/>> (February 23, 2003).

National Drug Intelligence Center. Federation of American Scientists. <<http://www.fas.org/irp/agency/doj/ndic/>> (February 23, 2003).

### SEE ALSO

*DEA (Drug Enforcement Administration) Drug Control Policy, United States Office of National Justice Department, United States*

cosmic rays, the space above Earth's atmosphere contains several hundreds of satellites and thousands of tons of space debris. Space debris orbiting the Earth consists of mostly non-functional man-made objects, many of which are fragments of satellites or rockets and residues from launches. On February 1, 2003, the space shuttle *Columbia* tragically ended its 16-day mission during its re-entry into Earth's atmosphere. One of the first questions that the scientific community investigated was whether *Columbia* had been struck by space debris.

There are about 600 active satellites orbiting the Earth. They are used for communication, remote sensing for weather, land surveys, national security, navigation, and support for scientific missions. These satellites are located in only a few orbital regions, mostly in the semisynchronous orbit, or the low Earth orbit (LEO) and the geosynchronous orbit (GEO). It is also in these regions where most of the space debris is located. The space debris around Earth not only poses risks to active satellites, but also to space missions and astronomical observations. Space debris is a major source of light pollution in wide-field imaging of astronomical objects.

One of the main problems associated with space debris is its duration, or lifetime. In contrast to meteoroids, which either burn in Earth's atmosphere or cross the near-Earth region to continue their travel through the solar system, space debris potentially can remain in orbit for millions of years. There are three issues of crucial importance in regards to space debris, namely how it can be cleaned up, how to avoid debris collisions with active spacecraft, and how to minimize the generation of more debris.

As early as the 1970s NASA began to investigate the feasibility of forcing space junk into the Earth's atmosphere, where remnants not destroyed by re-entry would fall to the ground. The central idea of this project, known as Orion, was to focus a high-powered laser beam into individual debris fragments, causing their outer layers to vaporize, and creating a thrust that would deflect their orbits. The research for the Orion project demonstrated that the clean-up would be extremely expensive, mainly because of the high power required by the laser and the high cost of the adaptive optics necessary to focus energy into small objects at great distances from the ground. This idea still might serve for the future, when technology may be able to equip satellites with the high-powered lasers and enable them to "sweep" space debris into the Earth's atmosphere.

There are two major risks from objects reentering the Earth's atmosphere. First, if they are too large to evaporate completely during re-entry, they could cause damage on the ground. Second, if the falling debris contains radioactive material, the atmosphere or ground could be contaminated. Currently, roughly 50 nuclear devices orbit the Earth, carrying a total of 1,300 kg (1.3 tons) of radioactive material. There have been at least two confirmed nuclear mishaps from space. In 1964, the orbit of an American satellite decayed into the Earth's atmosphere, releasing

---

## Near Space Environment

---

### ■ CECILIA COLOME

The near-Earth environment is far from empty. In addition to the natural meteoroid material, solar wind plasma, and

radioactive radiation over the Indian Ocean, and in 1978, a Soviet satellite lost its orbit and crashed in northern Canada, dispersing more than 30 kg (66.1 pounds) of enriched uranium. Nuclear reactors were very popular in space because they provide large energy sources in very small and lightweight volumes. All these devices were built and launched prior to 1988, and since then, nuclear reactors have not been incorporated into satellites.

As the density of the Earth's atmosphere decreases with altitude, objects in LEO experience more air friction than objects at higher altitudes. Over time, the orbits of non-functional objects decay to lower altitudes. The re-entry of large objects, with cross-sections of one square meter or more is significant; about one object re-enters daily, and some of them have survived the heat produced by re-entry air friction. Two notorious examples of debris re-entry are from the tanks belonging to a Delta rocket. In 1997, one of the tanks landed near a house, not far from a busy highway in Texas; a second tank from the Delta rocket landed in South Africa near Cape Town in 2000. To this date, there has been only one reported incident of a human being struck by space debris: in 1997, a woman in Tulsa, Oklahoma, was hit on the shoulder by a 6-inch piece of metal, and fortunately, it did not lead to any serious injury.

Both meteoroids and space debris pose a serious hazard to spacecraft and astronauts. The vast majority of meteoroids are small dust particles with typical sizes of tenths of a millimeter. Although they are small, due to their high speeds, up to 70 km/s, they represent a hazard in space. Current satellites are well shielded to withstand meteoroid impacts. Nevertheless, meteoroid collisions on spacecraft can be devastating for their operations. During a collision of a meteoroid, it evaporates partially or completely, and it may cause the evaporation of a small area of the external material on the spacecraft. The result is a plasma of electrons and ions. These particles are capable of inducing high electric currents on spacecraft, interfering with their basic control operations.

The dimensions of space debris cover a wide size range, from tiny dust particles to large non-functional rockets. Some of the main sources of space debris have been explosions of rockets. The collision avoidance with the larger (>10 cm, or >4 in) debris population is performed by tracking methods from the ground, either by radar or by optical measurements. Meteoroids are generally small, too small to be tracked reliably. Their potential collisions with spacecraft are taken into account in the shield design of spacecraft, and because they cannot be tracked, their collisions with active spacecraft can be treated only statistically. Ground-based radars are mostly used to monitor the space debris in LEO, while optical observations are used to track objects in GEO. Both methods have their own advantages and limitations. Radar measurements are not affected by weather nor day-night conditions, but because of their narrow bandwidths they cannot detect small objects at great distances. Optical tracking of space debris through telescopes requires the objects to be

illuminated by sunlight against a dark sky. In LEO, objects can be observed for only a few hours, but for objects in GEO, this method can be used during an entire night. Several countries are currently using radar and optical methods for tracking and making catalogues of space debris. Among them are England, France, Germany, Japan, Russia, Spain, and the United States.

The Haystack Auxiliary and Goldstone radars in the United States have provided ample data on the debris population with sizes smaller than 30 cm. The international collective effort has provided almost 9,000 catalogued large (>10 cm, or >4 in) objects. These catalogues are essential to avoid catastrophic collisions with active spacecraft. Three catalogues are updated regularly, one by the United States Space Command Satellite, one by the Russian Space Surveillance, and the other by the Information System Characterizing Objects in Space of the European Space Agency (ESA).

Explosions of spacecraft are considered to be the main source of large fragments of space debris. Part of the Pegasus rocket exploded in 1996, two years after its launch, creating 700 fragments large enough to be catalogued. The explosion of the Chinese Long March 4 rocket created more than 300 large fragments. At least three reported maneuvers of satellites have been performed in order to avoid collisions with space debris: both the European Remote Sensing Satellite (ERS-1) and the Satellite pour l'observation de la Terre (SPOT-2) in 1997, and the International Space Station (ISS) in 1999. A severe space accident occurred in 1996 when the French CERISE spacecraft was hit by a catalogued object, thought to be a fragment of the Ariane rocket's upper stage.

In order to gain better data on the space debris population, in 1984 the space shuttle *Challenger* deployed NASA's Long Duration Exposure Facility (LDEF). Its retrieval was scheduled for 1986, but due to the loss of the space shuttle *Challenger* it was postponed until 1990, when it was retrieved by *Columbia*. The LDEF orbited the Earth for almost 6 years, providing data on the near-Earth space environment, and returned to Earth covered by more than 30,000 craters. The LDEF was a large cylinder weighing more than 20,000 lbs, one of the heaviest objects deployed by any space shuttle. It contained 86 trays on its periphery where 57 experiments were carried out. These experiments were designed by NASA, the Department of Defense, universities and private companies, and were aimed for meteoroid and space debris studies, radiation surveys, and infrared video surveys. A major challenge in the study of the trays on LDEF was to distinguish between craters created by meteoroid impacts and those due to collisions with space debris, was accomplished by extensive chemical analysis. The data collected by LDEF had a major impact on the design of spacecraft after 1990. Most of the design changes involved the substitution of materials that deteriorate in space, such as Teflon, Kapton, Dracon, Mylar, and polymeric films. For example, the design of the radiator of the International Space Station was changed from Teflon to a ceramic paint. In general,

ceramic materials are better survivors of erosion due to bombardment of atomic oxygen and UV radiation.

One peculiar kind of potential space debris are tethers. Tethers are chains or ropes that connect astronauts to their spacecraft while working in space. They are also used as links between components on spacecraft. Tethers are a potential source of debris if they are discarded from spacecraft, but they also might help in the reduction of space debris. As a tether crosses the Earth's magnetic field lines, it becomes an electric generator. This energy source can be used not only to deploy spacecraft, but also to create the necessary thrust for lowering the altitude of non-functional objects. NASA has developed a unique experiment for future uses of tethers in space, The Propulsive Small Expendable Deployer System (ProSEDS), a thin wire 5 km long connected to a 10 km non-conductive rope. ProSEDS was scheduled for launch in 2003, and remains a high-priority for launch payload.

All effective clean-up procedures of space debris are still in experimental phases, although great advances have been made in slowing the increase of space debris with time. Spacecraft are now covered with longer lasting paints and their protective covers are much less affected by erosion by small meteoroids, particle bombardment, and UV radiation. Newer satellites are becoming increasingly smaller. This also reduces the probability of more generation of space debris, because the smaller the object is, the lower the probability of experiencing collisions.

#### ■ FURTHER READING :

##### BOOKS:

CETS. *Engineering Challenges to the Long-Term Operation of the International Space Station*. Washington, D.C.: The National Academies Press, 2000.

CPSMA. *Radiation and the International Space Station: Recommendations to Reduce Risk*. Washington, D.C.: The National Academies Press, 2000.

Gehrels, T., ed. *Hazards due to Comets & Asteroids*. Tempe, AZ: The University of Arizona Press, 1995.

Simpson, J. A., ed. *Preservation of Near-Earth Space for Future Generations*. New York: Cambridge University Press, 1994.

Tribble, A. C. *The Space Environment: Implications for Spacecraft Design*. Princeton: Princeton University Press, 1995.

##### PERIODICALS:

National Aeronautics and Space Agency. *Orbital Debris Quarterly News Letter*. Houston: Johnson Space Flight Center.

Revkin, Andrew C. "Wanted: Traffic Cops for Space." *New York Times*. February 18, 2003.

##### SEE ALSO

NASA (National Air and Space Administration)  
Satellites, Non-Governmental High Resolution  
Satellites, Spy

*Space Shuttle*  
*Strategic Defense Initiative and National Missile Defense*

## Nerve Gas

■ JUDYTH SASSOON

Nerve gases, or nerve agents, are mostly odorless compounds belonging to the organophosphate family of chemicals. Nerve gasses are either colorless or yellow-brown liquids under standard conditions. Two examples of nerve gases that have gained some notoriety through their powerful physiological effects are Sarin and VX. Even in small quantities, nerve gases inhibit the enzyme acetylcholinesterase and disrupt the transmission of nerve impulses in the body. Acetylcholinesterase is a serine hydrolase belonging to the esterase enzyme family, which acts on different types of carboxylic esters in higher eukaryotes. Its role in biology is to terminate nerve impulse transmissions at cholinergic synapses. It does this by rapidly hydrolysing the neurotransmitter, acetylcholine, which is released at the nerve synapses. Inhibition of the acetylcholinesterase results in the excessive buildup of acetylcholine in, for example, the parasympathetic nerves leading to a number of important locations in the body: the smooth muscle of the iris, ciliary body, the bronchial tree, gastrointestinal tract, bladder and blood vessels; also the salivary glands and secretory glands of the gastrointestinal tract and respiratory tract; and the cardiac muscle and endings of sympathetic nerves to the sweat glands. An accumulation of acetylcholine at parasympathetic sites gives rise to characteristic muscarinic signs, such as emptying of bowels and bladder, blurring of vision, excessive sweating, profuse salivation and stimulation of smooth muscles. The accumulation of acetylcholine at the endings of motor nerves leading to voluntary muscles ultimately results in paralysis.

Nerve gases are highly toxic, stable, and easily dispersed. They produce rapid physiological effects both when absorbed through the skin or through the respiratory tract. They are also fairly easy to synthesize and the raw materials required for their manufacture are inexpensive and readily available. This means that anyone with a basic laboratory can produce them. Nerve gases are, therefore, a significant concern for authorities as they are an easily available weapon for terrorist groups.

In 1936, the German chemist Gerhard Schrader of the I. G. Farbenindustrie laboratory in Leverkusen first prepared the agent Tabun (ethyl-dimethylphosphoramidocyanidate). At the time, Schrader was leading a program to develop new types of insecticides, working first with fluorine-containing compounds such as acyl fluorides, sulfonyl fluorides, fluoroethanol derivatives and fluoroacetic acid derivatives. Schrader's research eventually led to the synthesis of Tabun as an extremely powerful



Cold War-era artillery shells containing GB nerve gas are carefully loaded into a steel cask for transport to an incinerator at a chemical depot in Utah in 2001. AP/WIDE WORLD PHOTOS.

agent against insects. Schrader found that as little as 5 parts per million (ppm) of Tabun killed all the leaf lice used in his experiments. Soon after Schrader's experiments, the potential use of this substance as an agent of war was realized.

In 1939, a pilot plant for Tabun production was set up at Munster-Lager, near the German Army training grounds at Raubkammer. In January 1940, Germany began the construction of a full-scale plant, code named Hochwerk, at Dyernfurth-am-Oder (now Brzeg Dolny in Poland). A total of 12,000 tons of Tabun was produced during the ensuing three years (1942–1945) and at the end of WWII, large quantities were seized by the Allied Forces. In addition to Tabun, Schrader and his colleagues produced some 2000 new organophosphates, including Sarin in 1938 and the third of the "classic" nerve agents, Soman, in 1944. These three nerve agents, Tabun, Sarin and Soban,

are known as G-agents. The manufacture of Sarin was never fully developed in Germany and only about 0.5 tons were produced in a pilot plant before the end of WWII in 1945.

After 1945, a great deal of research began to focus on understanding the physiological mechanisms of nerve gas action, so that more effective means of protection could be devised against them. However, these efforts also allowed for the development of new and more powerful agents, closely related to the earlier ones. The first official publications on these compounds appeared in 1955. The authors, British chemists Ranajit Ghosh and J. F. Newman, described Amiton, one of the newly developed nerve agents, as being particularly effective against mites. At this time, researchers were devoting a great deal of energy to studying organophosphate insecticides both in Europe and in the United States. At least three chemical firms independently studied and quantified the intense toxic properties of these compounds during the years 1952–53 and some of them became available on the market as pesticides. By the mid-1950s, following in the wake of the intensive research activity, a new group of highly stable nerve agents had been developed. These were known as the V-agents and were approximately ten-fold more poisonous than Sarin. The V-agents can be numbered among the most toxic substances ever synthesized. VX, a persistent nerve gas, was discovered by Ghosh and was touted as being more toxic than any previously synthesized compound. Since the discovery of VX, there have been only minor advancements in the development of new nerve agents.

A contemporary use of nerve gas occurred during the Iran-Iraq war of 1984–1988. In this conflict, the United Nations confirmed that Iraq used Tabun and other nerve gases against Iran. This incident is a prime example of how the technology of chemical weapons was shared during the Cold War. The Soviets would arm their allies while the U.S. did the same for its allies. Iraq was a benefactor and implemented its chemical stockpiles during this period. Another contemporary incident of nerve gas use occurred in Japan in 1995. Members of the Aum Shinrikyo cult introduced Sarin gas into Tokyo's subway system. This incident gives an example of the possible new roles that nerve gases may play in the future, as tools of terrorism rather than the weapons of powerful nations.

#### ■ FURTHER READING:

##### BOOKS:

- Paxman, J., and R. Harris. *A Higher Form of Killing: The Secret Story of Chemical and Biological Warfare*. New York: Hill and Wang, 1982.
- Poolos, J. *Nerve Gas Attack on the Tokyo Subway*. Rosen Publishing Group Inc., 2002.
- Stockholm International Peace Research Institute. *The Problem of Chemical and Biological Warfare. A Study of the Historical Technical, Military, Legal, and Political Aspects of CBW and Possible Disarmament Measures*.

Vol. 1. *The Rise of CB Weapons*. New York: Humanities Press, 1971.

#### PERIODICALS:

Evison D, D. Hinsley, and P. Rice. "Chemical Weapons." *BMJ* 324 (2002): 332–335.

Yergler, M. "Nerve Gas Attack." *Am. J. Nurs.* 1 (2002): 57–60.

#### ELECTRONIC:

Lenthall, Joe. University of Oxford. "Molecule of the month, VX gas." <<http://www.chem.ox.ac.uk/mom/vx/VX.htm>> (February 20, 2003).

#### SEE ALSO

*Chemical and Biological Defense Information Analysis Center (CBIAC)*

*Chemical and Biological Detection Technologies*

*Chemical Biological Incident Response Force, United States*

*Chemical Warfare*

*Chemistry: Applications in Espionage, Intelligence, and Security Issues*

*Terrorist Threat Integration Center*

#### NEST Team.

SEE *Nuclear Emergency Support Team, United States.*

---

## Netherlands, Intelligence and Security

---

The Kingdom of the Netherlands was established following the Napoleonic Wars in 1815. Since its founding, the Netherlands has been influential in international politics, but has long maintained a policy of stated neutrality. Despite their officially neutral position, the Netherlands was invaded and occupied by Nazi forces during World War II. Though the Queen and many government officials fled to Britain before the invasion, the Dutch people formed secret resistance groups and refugee smuggling networks, many led by members of the Dutch intelligence community.

After World War II, the Netherlands reformed several government agencies, including the intelligence and security services. The Dutch government strengthened the intelligence community, and its accountability to government officials. Separate civilian and military intelligence services were created, but were designed to work in cooperation with each other. Today, the Netherlands is a member of the European Union, and hosts the international courts of the United Nations.

The main civilian intelligence agency is the *Algemene Inlichtingen -en Veiligheidsdienst* (AIVD), or the General Intelligence and Security Service. The agency conducts all means of intelligence operations, but focuses on domestic intelligence. The AIVD is charged with the protection of domestic security and assessment of threats to Dutch interests within its national and territorial borders. The agency analyzes all intelligence information, and reports threats and other security issues to government officials.

The Netherlands established their military intelligence service immediately before the outbreak of World War I maintained those services, even operating clandestinely during the World War II Nazi occupation. The current, primary, Dutch military intelligence agency is the *Militaire Inlichtingendienst* (MID), or Military Intelligence Agency. The Ministry of Defense, Ministry of Justice, and the Ministry of Affairs all contribute to the administration of the MID. Though foreign intelligence and external security issues are the primary focus of the MID, the agency also conducts strategic communications, economic, technological, and limited political intelligence operations. The agency maintains a counter-terrorism and counter espionage force, the Counter Intelligence Task Bureau, (CIV). Securing military and government interests and guarding them from espionage are the chief concerns of the CIV.

Dutch intelligence works closely with allies in the European Union and the North Atlantic Treaty Organization (NATO). In addition to supporting international intelligence efforts to halt weapons proliferation and fight global terrorism, the Dutch intelligence and security communities also protect significant United Nations interests in The Hague.

#### SEE ALSO

*European Union*

*World War II*

#### Neural Network Based Optics.

SEE *Brain-Machine Interfaces.*

---

## New People's Army (NPA)

---

The New People's Army (NPA) is the military wing of the Communist Party of the Philippines (CPP). A Maoist group formed in March, 1969, its aim includes overthrowing the Philippine government through protracted guerrilla warfare. The chairman of the CPP's Central Committee and the NPA's founder, Jose Maria Sison, directs all CPP and NPA activity from the Netherlands, where he lives in self-imposed exile. Fellow Central Committee member and director of the CPP's National Democratic Front (NDF) Luis

Jalandoni also lives in the Netherlands and has become a Dutch citizen.

Although primarily a rural-based guerrilla group, the NPA has an active urban infrastructure to conduct terrorism and uses city-based assassination squads. The NPA derives most of its funding from contributions of supporters in the Philippines, Europe, and elsewhere, and from so-called "revolutionary taxes" extorted from local businesses.

The NPA primarily targets Philippine security forces, politicians, judges, government informers, former rebels who wish to leave the NPA, and alleged criminals. NPA opposes any U.S. military presence in the Philippines, and before the base closures in 1992 attacked U.S. military installations. Press reports in 1999 and in late 2001 indicated that the NPA is again targeting U.S. troops participating in joint military exercises as well as U.S. Embassy personnel. The NPA claimed responsibility for the assassination of congressmen from Quezon and Cagayan and many other killings. NPA strength is estimated at over 10,000. NPA operates in rural Luzon, Visayas, and parts of Mindanao with cells in Manila and other metropolitan centers.

#### ■ FURTHER READING:

##### ELECTRONIC:

CDI (Center for Defense Information), Terrorism Project.

CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <<http://www.cdi.org/terrorism/terrorist.cfm>> (April 17, 2003).

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001," Annual Report: On the Record Briefing. May 21, 2002. <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual Reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

##### SEE ALSO

*Terrorism, Philosophical and Ideological Origins*  
*Terrorist and Para-State Organizations*  
*Terrorist Organization List, United States*  
*Terrorist Organizations, Freezing of Assets*

---

## New Zealand, Intelligence and Security

---

New Zealand gained its independence from Britain in 1907, but remains a member of the British Commonwealth. A longtime, close ally with Britain, Australia, and

the United States, New Zealand retreated from international politics during the last two decades to address ethnic tensions between European-descended New Zealanders and the native Maori people. The New Zealand government strived to recognize past aggression against the Maori community, reforming national government and social policy to address native grievances. As part of these reforms, the New Zealand government declassified information gained from past surveillance of Maori populations.

The Security Intelligence Service (SIS) is New Zealand's primary civilian intelligence agency. Charged with the gathering, processing, and analyzing of foreign and domestic intelligence, the SIS conducts a wide-variety of intelligence operations. The agency maintains a small human intelligence force, choosing to gather information from carefully negotiated liaisons with allied foreign intelligence services, such as those of Britain, the United States, and Australia. The main mission of the SIS is the protection of New Zealand's national, military, economic, technological, and scientific infrastructure.

The Government Communications Security Bureau (GCSB) limits its operations to foreign intelligence and counter-intelligence operations. The bureau supervises the protection of government communications, computer, and information systems. The agency also processes collected foreign intelligence information for dissemination to international intelligence and security agencies.

New Zealand's civilian intelligence community is administered by the Office of the Prime Minister and the Cabinet Strategy Subcommittee on Intelligence and Security (CSSIS). The CSSIS has limited power to mobilize military responses to identified threats against national interests. In most cases, however, the CSSIS relies on the New Zealand Parliament to authorize the use of force.

In addition to civilian intelligence forces, New Zealand also maintains substantial military intelligence forces. Special intelligence units are embedded in the operations divisions of the various branches of service. Since these units focus on strategic intelligence, the military works closely with civilian agencies to gather and analyze intelligence. New Zealand's Naval Intelligence is the largest military intelligence organization, specializing in signals, communications, and remote intelligence operations in the South Pacific.

In 2001, New Zealand's intelligence community pledged to support global anti-terrorist operations. The strategic position of New Zealand in the Austral-Asian South Pacific facilitates remote intelligence and surveillance operations in the region. New Zealand often contributes intelligence regarding the ongoing conflict in Indonesia to the United Nations and other international security agencies.

##### SEE ALSO

*Australia, Intelligence and Security*  
*United Kingdom, Intelligence and Security*

---

## NFIB (United States National Foreign Intelligence Board)

---

The National Foreign Intelligence Board (NFIB) was created by the National Security Act of 1947. The NFIB acts as a communications channel among various national intelligence agencies and facilitates interagency exchange of information. The board also develops policy regarding the protection of intelligence information. In addition to coordinating domestic matters, the board also handles relationships with foreign intelligence agencies that share information with the United States and allocates that information to the appropriate U.S. agencies.

The NFIB is chaired by the Director or Deputy Director of Central Intelligence. In permanent membership, all agencies within the United States intelligence and federal law enforcement community are represented on the committee, as well as the Departments of Energy and Treasury. Other agencies are occasionally represented on the board. Representatives from the Department of the Interior and the Department of Health and Human Services sometimes join the board to discuss counter-terrorism measures, but are not permanent sitting members of the NFIB. The major subsidiary committee of the NFIB is the National Intelligence Council, which coordinates intelligence studies and analyses of various issues, threats, or locations.

While the board was created to address the transfer of information regarding military and political national security threats, the NFIB has become increasingly interested in the role of the intelligence community in the preservation and regulation of international economic interests. The Department of Treasury was added to the NFIB in 1972 to foster links between monetary policy makers, banks, international funds and economic cooperatives and intelligence agencies.

Upon full implementation of the Department of Homeland Security, the NFIB will be restructured to include, be governed by, or be replaced by the new agency. Since the new Homeland Security Department is will perform many of the same functions as the older interagency committee, the future structure and role of the NFIB has yet to be fully determined.

---

## NIC (National Intelligence Council)

---

The National Intelligence Council (NIC) oversees the estimative process of the United States intelligence community, and produces National Intelligence Estimates

(NIEs). The NIC answers directly to the Director of Central Intelligence (DCI) in his capacity as head of the intelligence community. In addition to producing NIEs, NIC generates other reports, and avails itself of knowledge provided by civilian experts through its Global Expertise Reserve Program (GERP).

**Mission and organization.** NIC is the principal intelligence community center for mid-term and long-term strategic analysis. Among its principal functions are supporting DCI as leader of the intelligence community; providing a tasking office whereby policymakers may present requests for information to members of the intelligence community; drawing on the expertise of non-government authorities in academia and the private sector, so as to broaden the intelligence community's perspective on issues of importance; and leading in the production of NIEs and other informational products.

NIC has several national intelligence officers (NIOs) focused on geographic areas or specific issues regarding national security and intelligence. As of 2003, it had NIOs devoted to Africa, conventional military issues, east Asia, economics and global issues, Europe, Latin America, the Near East and south Asia, Russia and Eurasia, science and technology, strategic and nuclear programs, and warnings. In addition, there was an at-large NIO.

NIOs have the responsibility of advising the DCI, supporting the needs of senior intelligence consumers, producing estimative intelligence, tapping the knowledge and insights of outside experts, helping to assess the capabilities of intelligence community analytic producers, promoting collaboration between producers of analysis within the intelligence community, and articulating priorities to guide future efforts in intelligence collection, evaluation, and procurement.

**NIC products and programs.** By far the most significant NIC product is the NIE, which dates back to the intelligence failures of the late 1940s—particularly the miscalculations of Chinese and North Korea intentions on the Korean peninsula that led to the surprise invasion of South Korea in 1950. Responding to these failures, General Walter Bedell Smith, upon becoming DCI in October, 1950, created the NIE as a means of drawing upon the expertise of the entire intelligence community. In addition to the NIE, NIC has produced studies and reports such as “Transformations in Defense Markets and Industries,” issued in late summer 2001. The report noted two trends in national armament policies: on the one hand, governments were broadening the range of sources from which they purchased weapons, and on the other hand, national defense industries were competing to export arms to other nations. These trends were creating “a world characterized by the routine diffusion of weapons and technology.”

In December, 2000, NIC issued an enormous report titled *Global Trends 2015: A Dialogue About the Future*

with *Nongovernment Experts*. The report identified seven key factors that would shape the world over the next 15 years, and made specific predictions, for instance suggesting the strong possibility of international conflict over water rights and access to fresh water. Among the larger trends cited in the report were scientific and technological advances, changes in the nature of military power and conflict, globalization of markets, and increased conflict over oil and other energy sources.

**GERP.** Many of the NIC's products are a result of GERP, through which it has sought to expand the reach of the intelligence community by fostering dialogue between intelligence analysts and non-government experts. Reservists, as participants in GERP are called, come from academia, the corporate world, and private think tanks. They are typically U.S. citizens who have traveled widely, and who have closely followed a particular topic or geographic area of interest for at least 10 years. As NIC noted on its Web site in 2003, "In the past, topics covered by the Reserve have ranged from stability and conflict in sub-Saharan Africa, to the impact of organized crime in the Caribbean, to economic growth in Iran."

Participation in GERP, as NIC also noted, "is not about being 'James Bond'"; in other words, reservists serve purely in the role of consultants, and are not involved in the collection of intelligence, or in other covert activities. Nor are they called upon to take any action on behalf of the federal government. Rather, their role is simply to participate with NIC as consultants. All reservists are paid for their work, and some are placed on retainer, while others are consulted on a case-by-case basis. They are expected to maintain confidentiality as appropriate, but outside of restrictions relating to national security, they are free to publish.

#### ■ FURTHER READING:

##### PERIODICALS:

Nye, Joseph S., Jr. "Peering into the Future." *Foreign Affairs* 73, no. 4 (July/August 1994): 82.

Postel, Sandra L., and Aaron T. Wolf. "Dehydrating Conflict." *Foreign Policy* no. 126 (September/October 2001): 60–67.

Wall, Robert. "New Arms Policies Seen Altering Warfare." *Aviation Week & Space Technology* 155, no. 10 (September 3, 2001): 100.

Zelikow, Philip. "The Global Infectious Disease Threat and Its Implications for the United States." *Foreign Affairs* 79, no. 4 (July/August 2000): 154–155.

##### ELECTRONIC:

Global Trends 2015: A Dialogue About the Future with Nongovernment Experts. Central Intelligence Agency. <<http://www.cia.gov/cia/publications/globaltrends2015/>> (March 17, 2003).

National Intelligence Council. <<http://www.cia.gov/nic/>> (March 17, 2003).

#### SEE ALSO

*DCI (Director of the Central Intelligence Agency) Intelligence Community*  
*Nongovernmental Global Intelligence and Security*

## Nicaragua, Intelligence and Security

Nicaragua gained independence from Spain in 1821, and became a republic in 1838. Late-twentieth-century politics in the region have been marked by violence and turmoil. A brief civil war in 1979 ushered the Marxist Sandinistas to power. Cold War politics, and Sandinista military aid to other leftist rebel groups in the region, prompted the United States to assist anti-Sandinista, contra forces. By the end of 1989, the Sandinistas had lost control of much of Nicaragua, but not before continued violence, rampant corruption, and the actions of secret police forces had devastated the nation.

Domestic intelligence is the responsibility of the Directorate of Intelligence Affairs (DAI). The DAI does conduct limited foreign intelligence operations and processes most of the information gathered by other Nicaraguan intelligence forces. The chief officers of the DAI, as well as members of the Ministry of the Interior, act as a liaison between the intelligence community and the government executive. The relationship between the intelligence community and the government is somewhat ambiguous, with no formal means of accountability or a standardized oversight process. Even following the recent democratic elections, the DAI has come under increasing scrutiny for political espionage activities.

Nicaragua's main military intelligence agency is the Directorate of Military Intelligence. The agency coordinates military and foreign intelligence operations, but also conducts surveillance of paramilitary and opposition groups in the region. The routine operations of the Directorate of Military Intelligence remain largely unknown, but the organization has close ties to political officials and the civilian intelligence community.

Nicaraguan free elections in 1990, 1996, and 2001 ousted the Sandinistas from power, but economic and political recovery has been difficult. Drug trafficking and corruption remain endemic problems, and years of guerrilla fighting have left many Nicaraguans with a deep distrust of the government, military, and other security forces.



Nicaragua is a member of the United Nations (UN) and several other Central and Latin American defense and economic organizations. The government has joined international efforts to stem drug trafficking, combat illegal arms sales, and fight global terrorism.

#### ■ FURTHER READING :

##### ELECTRONIC:

Central Intelligence Agency. "Nicaragua." CIA World Factbook. <<http://www.cia.gov/cia/publications/factbook/geos/nu.html>> (April 8, 2003).

## Nigeria, Intelligence and Security

In 1998, Nigeria overthrew its ruling dictatorship, which possessed close ties to the nation's military. The transitional government that gained power attempted to restore the long-suspended Constitution of 1979 and institute democratic reforms. The progress of reform has been slow.

The Nigerian intelligence community was an instrumental part of the former authoritarian regime. Political espionage, surveillance of citizens, and detainment of political dissidents was commonplace, garnering criticism for its brutality from the international community.

Nigeria's intelligence community was radically restructured in 1986. The National Security Organization was dissolved, prompting the formation of three, smaller, more specialized agencies. The National Intelligence Agency (NIA) is Nigeria's main civilian intelligence agency. The main responsibilities of the NIA are counterintelligence and foreign intelligence collection operations. The NIA focuses on external threats to Nigerian national interests. The State Security Service (SSS) manages domestic intelligence, and works closely with the Federal Investigation and Intelligence Bureau (FIIB), the liaison agency between law enforcement and intelligence services.

Nigeria's military intelligence is also coordinated through the executive office of the government. The Defense Intelligence Agency (DIA) is responsible for foreign and domestic military intelligence. The DIA is more secretive in its operations and maintains a larger special action force than the civilian intelligence agencies.

Democratic reforms have progressed slowly in Nigeria. Government corruption remains endemic. Despite changes made to the Nigerian intelligence community, political espionage and abuse of intelligence resources

are still reported by Western human rights agencies, which claim that accusations of the rape and torture of citizens along with destruction of private property increased in 2002. Human rights agencies and western intelligence service reports maintain that Nigerian government censorship of media and communications, including the use of intelligence resources for surveillance, persists.

Nigeria is the most populous nation in Africa. The nation's major export is oil, which provides the government with over half of its annual income. In 2002, Nigeria was the fifth largest oil supplier to the United States.

## Night Vision Scopes

■ LARRY GILMAN

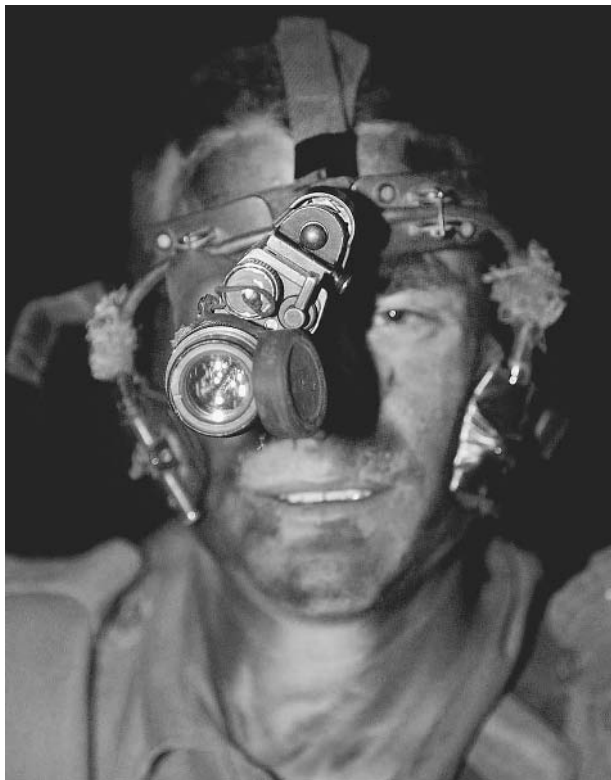
Night vision scopes are devices that enable machines or people to "see in the dark," that is, to form images when illumination in the visible band of the electromagnetic spectrum is inadequate. Although it is not possible to form images in *absolute* darkness, that is, in the absence of any electromagnetic radiation whatsoever, it is possible to form images from radiation wavelengths to which the human eye is insensitive, or to amplify visible-light levels so low that they appear dark to the human eye.

There are two basic approaches to imaging scenes in which visible light is inadequate for human vision:

(1) Low-level visible light that is naturally present may be amplified and presented directly to the viewer's eye. (Light in the near-infrared part of the electromagnetic spectrum [ $>.77-1.0$  microns], either naturally present or supplied as illumination, may also be amplified and its pattern translated into a visible-light pattern for the viewer's benefit.) This technique is termed image intensification.

(2) Light in the infrared part of the spectrum ( $>.8$  microns) is emitted by all warm objects and may be sensed by electronic devices. A visible-light image can then be produced for the user's benefit on a video screen. This technique is termed thermal imaging.

**Image intensification.** Image intensification, the method used for the devices termed night-vision scopes, exist in a variety of forms and can be mounted on weapons or vehicles or worn as goggles by an individual. Image-intensification devices have been used by technologically advanced military organizations since the 1950s. In a modern, high-performance light amplifier, light from the scene is collimated—forced to become a mass of parallel rays—by being passed through a thin disk comprised of thousands of short, narrow glass cylinders (optical fibers)



An Israeli soldier checks his night vision equipment at an Israeli army base in the Jewish settlement of Avnei Hefetz in March, 2002. AP/WIDE WORLD PHOTOS.

packed side by side. The parallel rays of light emerging from these optical fibers are directed at a second disk of equal size, the microchannel plate. The microchannel plate is also comprised of thousands of short, narrow cylinders (.0125-mm diameter, about one fourth the diameter of a human hair), but these microchannels are composed of semiconducting crystal rather than optical fiber. A voltage difference is applied between the ends of each microchannel. When a photon (the minimal unit of light, considered as a particle) strikes the end of a microchannel, it knocks electrons free from the atoms in the semiconducting crystal. These are pulled toward the voltage at the far end of the microchannel, knocking more electrons loose as they move through the crystal matrix. Thousands of electrons can be produced in a microchannel by the arrival of a single photon. At the far end of the microchannel, these electrons strike a phosphor screen that is of the same size and shape as the microchannel disk. The phosphor screen contains phosphor compounds that emit photons in the green part of the visible spectrum when struck by electrons; thus, that part of the phosphor disk affected by a single microchannel glows visibly, the brightness of its glow being in proportion to the intensity of the electron output of the microchannel. (Green is chosen because the human eye can distinguish brightness variations in green more efficiently than in any other

color.) The phosphor-disk image is comprised of millions of closely packed dots of light, each corresponding to the electron output of a single microchannel. The light from the phosphor disk is collimated by a second fiber-optic disk and presented to the viewer's eye through a lens. The function of the lens is to allow the user's eye to relax (i.e., focus at infinity), rather than straining to focus on an image only an inch or so away. Alternatively, the phosphor-disk image can be filmed by a camera.

A pair of night-vision goggles may contain two such systems, either one for each eye, or, as in the case of the U.S. Army's AN/PVS-7B night vision goggles, a single image may be split into identical copies and presented to both the user's eyes simultaneously.

A "third generation" image intensifier has been described above; several other image-intensification technologies remain in the field. All, however, operate by using photons to liberate electrons, amplifying the resulting electron current, and using the amplified electron current to liberate visible photons.

Image intensifiers form sharp images with natural contrast patterns. Also, they use very little power and so can run for many hours on, say, a battery mounted in a helmet. Because they are relatively cheap and can provide a mobile individual with the ability to see in most "dark" conditions, hundreds of thousands of night-vision goggles and scopes based on image intensification have been sold to military and police forces worldwide. Criminals have also been using them increasingly, as a number of models are now available on the consumer market. However, night-vision goggles provide poor peripheral vision, which can disorient pilots or drivers. Further, they cannot work in settings where visible and near-infrared light are truly absent (e.g., inside a windowless building). The latter disadvantage can only be partly offset by providing active illumination (e.g., a laser), because such light sources reveal themselves to enemy forces equipped with image intensifiers.

**Infrared imaging.** Image intensification amplifies radiation *reflected* by objects; infrared imaging works by detecting radiation *emitted* by objects. All objects at non-cryogenic temperatures glow spontaneously in the infrared region of the spectrum. Air is opaque to some of this radiation, but has two wavelength "windows" through which infrared radiation passes freely: the 3–5 micron window and the 8–12 micron window. (One micron is a millionth of a meter.)

Semiconductor devices sensitive to infrared radiation in either of the two atmospheric infrared windows can be built, in large numbers, on the surface of a chip. An infrared image focused on the surface of such an array can be read off electronically as image information, which is then used to construct a visible-light image on a screen.

Infrared imaging systems are bulkier and more expensive than image intensification systems. However, they

work even in a complete absence of illumination (since all scenes “glow” in infrared) and can detect otherwise invisible phenomena, such as hot, nonsmoky exhaust plumes or buried landmines, that may be of military or security interest. Infrared imagers are also used for a wide variety of forensic and industrial purposes, as they can reveal chemical compositional differences not evident in visible light.

## ■ FURTHER READING:

### BOOKS:

Schlessinger, Monroe. *Infrared Technology Fundamentals*. New York: Marcel Dekker, Inc., 1995.

### PERIODICALS:

Owens, Ken, and Larry Matthies. “Passive Night Vision Sensor Comparison for Unmanned Ground Vehicle Stereo Vision Navigation,” in proceedings from the *International Conference on Robotics and Automation*. (2000): 122–131.

Thompson, R. J. “New Developments in Night-Vision Equipment and Techniques,” in proceedings from the *1995 International Carnahan Conference on Security Technology*. (2000): 144–446.

research scientists, and promotes the spread of medical information. Funds for the NIH are appropriated from Congress. In 2002, the NIH was appropriated almost \$23.4 billion. Research grants for non-federal scientists account for about 84 percent of the appropriation. NIH’s in-house research accounts for about 10 percent of the appropriation. The remainder of the budget goes toward research support costs.

NIH is one of the agencies of the Public Health Service, which is a component of the Department of Health and Human Services. NIH is comprised of 27 institutes and centers:

- Center for Information Technology
- Center for Scientific Review
- John E. Fogarty International Center
- National Cancer Institute
- National Center for Complementary and Alternative Medicine
- National Center on Minority Health and Health Disparities
- National Center for Research Resources
- National Eye Institute
- National Heart, Lung, and Blood Institute
- National Human Genome Research Institute
- National Institute on Aging
- National Institute on Alcohol Abuse and Alcoholism
- National Institute of Allergy and Infectious Diseases
- National Institute of Arthritis and Musculoskeletal and Skin Diseases
- National Institute of Biomedical Imaging and Bioengineering
- National Institute of Child Health and Human Development
- National Institute on Deafness and Other Communication Disorders
- National Institute of Dental and Craniofacial Research
- National Institute of Diabetes and Digestive and Kidney Diseases
- National Institute on Drug Abuse
- National Institute of Environmental Health Sciences
- National Institute of General Medical Sciences
- National Institute of Mental Health
- National Institute of Neurological Disorders and Stroke
- National Institute of Nursing Research
- National Library of Medicine
- Warren Grant Magnuson Clinical Center

## NIH (National Institutes of Health)

### ■ BELINDA ROWLAND

The National Institutes of Health (NIH) is a federal agency that serves as the fiscal agent of medical research in the United States. The mission of the NIH is to foster medical and behavioral research on living systems and to use that knowledge to prevent, identify, diagnose, and treat illness and disability.

The NIH originated in 1887 as a one-room bacteriological laboratory on Staten Island that was called The Hygienic Laboratory. The Hygienic Laboratory was established by the Marine Hospital Service (The Public Health Service) to diagnose and study bacterial epidemics. This laboratory marked the beginning of government-supported medical research in the United States. The Laboratory’s name was changed to the National Institutes of Health in 1930. In 1938, the NIH moved to its present location in Bethesda, Maryland.

As the primary medical research agency in the United States, NIH conducts research in its own laboratories, allocates research funds for non-federal scientists, trains

**The role of NIH in a national health crisis.** The NIH would play a crucial role in the event of a national health crisis.

The appropriate institutes within NIH would be called upon to conduct and support research that is relevant to the crisis at hand. NIH policy and the planning and management of all NIH activities is the responsibility of the Office of the Director. The Department of Homeland Security integrates many of the government's agencies to protect the American people from potential threats.

United States President George W. Bush is committed to providing a large appropriation to NIH to support biological terrorism research. In the wake of the September 11, 2001 attacks, the National Institute of Allergy and Infectious Diseases (NIAID) and the National Institute of Mental Health (NIMH), which are institutes within NIH, were called into action. NIAID has supported much of the research into the prevention, diagnosis, and treatment of illnesses caused by microorganisms that may be used by bioterrorists. Immediately after the October 2001 bioterrorist attacks, NIAID accelerated the research of bacteria and viruses that the Centers for Disease Control and Prevention (CDC) classifies as "Category A" agents. Category A agents are microorganisms that cause severe illness and high death rates and are easy to spread.

NIMH has provided information and counseling to Americans who were trying to cope with the September 11, 2001 terrorist attacks. They support the survivors, emergency personnel, and millions of others who were directly or indirectly affected by the attacks.

#### ■ FURTHER READING:

##### BOOKS:

- Kondratas, R. *Images from the History of the Public Health Service*. U.S. Department of Health and Human Services, Public Health Service, 1994.
- Kurian, G. T., ed. *A Historical Guide to the U.S. Government*. New York: Oxford University Press, 1998.
- Mullan, F. *Plagues and Politics: The Story of the United States Public Health Service*. New York: Basic Book, Inc., 1989.
- Wilcox, W. *Public Health Sourcebook: Basic Information About Government Health Agencies*. Detroit: Omnigraphics, 1998.

##### ELECTRONIC:

- National Institutes of Health, 9000 Rockville Pike, Bethesda, Maryland 20892. <<http://www.nih.gov>> (January 1, 2003).
- Office of the Public Health Service Historian, 18-23 Parklawn Building, 5600 Fishers Lane, Rockville, Maryland, 20857. (301) 443-5363. August 21, 2000. <<http://lhncbc.nlm.nih.gov/apdb/phsHistory>> (October 19, 2000).

##### SEE ALSO

*Bioterrorism*  
 CDC (United States Centers for Disease Control and Prevention)

*Health and Human Services Department, United States Homeland Security, United States Department of Microbiology: Applications to Espionage, Intelligence and Security*  
 NIMH (National Institute of Mental Health)  
 Public Health Service (PHS), United States  
 September 11 Terrorist Attacks on the United States

## NIJ (National Institute of Justice)

The National Institute of Justice (NIJ) serves the United States Department of Justice in the areas of research, development, and evaluation. Established under the authority of the Omnibus Crime Control and Safe Streets Act of 1968, its purpose is to provide independent, evidence-based tools to assist state and local law enforcement. Its programs address a variety of law-enforcement issues, including use of DNA evidence, drug abuse, and domestic violence.

Appointed by the President and confirmed by the Senate, the director of NIJ is responsible for establishing objectives in alignment with Justice Department priorities, as well as the current needs of the field. It works to take account of views from professionals in all areas of criminal justice and related fields in its search for knowledge and tools to guide the policy and practice of law enforcement nationwide. On January 12, 2003, it reorganized, streamlining its structure from three offices to two; the Office of Development and Communications and the Office of Research and Evaluation.

NIJ has set research priorities in a number of fields, including law enforcement and policing; justice systems (sentencing, courts, prosecution, defense); corrections; investigative and forensic sciences (including DNA); counterterrorism and critical incidents; crime prevention/causes of crime; violence and victimization (including violent crimes); drugs, alcohol, and crime; interoperability, spatial information, and automated systems; and program evaluation. Among its programs are the Arrestee Drug Abuse Monitoring Program (ADAM); Community Mapping, Planning, and Analysis for Safety Strategies (COMPASS); National Commission on the Future of DNA Evidence; and the Violence Against Women and Family Violence Research and Evaluation Program.

#### ■ FURTHER READING:

##### BOOKS:

Connors, Edward F. *Convicted by Juries, Exonerated by Science: Case Studies in the Use of DNA Evidence*

to *Establish Innocence After Trial*. Washington, D.C.: National Institute of Justice, 1996.

Kelling, George L. *Broken Windows and Police Discretion*. Washington, D.C.: National Institute of Justice, 1999.

Riley, Kevin Jack. *Crack, Powder Cocaine, and Heroin: Drug Purchase and Use Patterns in Six U.S. Cities*. Washington, D.C.: National Institute of Justice, 1998.

#### PERIODICALS:

"Crime Year in Review." *Crime Control Digest* 36, no. 35 (August 30, 2002): 1.

"NIJ Technologies for Public Safety." *Law & Order* 50, no. 8 (August 2002).

Waldron, Ronald J. "National Institute of Justice Helps Facilities Implement Telemedicine Program." *Corrections Today* 64, no. 2 (April 2002): 184.

#### ELECTRONIC:

National Institute of Justice. <<http://www.ojp.usdoj.gov/nij/>> (March 28, 2003).

#### SEE ALSO

*DNA Fingerprinting*  
*Justice Department, United States*  
*Law Enforcement, Responses to Terrorism*

---

## NIMA (National Imagery and Mapping Agency)

---

The National Imagery and Mapping Agency (NIMA) was formed in October, 1996, to provide the United States military and intelligence agencies with up-to-date and accurate imaging and geospatial information. NIMA is a Department of Defense agency and is a member of the United States intelligence community. NIMA uses satellite and aerial imaging equipment to produce maps that can be used by both military planners and soldiers in the field.

NIMA assumed the duties of the Defense Mapping Agency, the Central Imagery Office, the Defense Dissemination Program Office, the National Photographic Interpretation Center, and parts of the Defense Intelligence Agency, the National Reconnaissance Office (NRO), Defense Airborne Reconnaissance Office, and the Central Intelligence Agency. NIMA now serves as the sole source for mapping and imaging needs of the U.S. military and intelligence agencies.

NIMA uses satellite photographic, radar, and infrared imaging information to create and analyze a database of cartographic and geodetic images. NIMA can then customize these images to suit the needs of its customers.

NIMA's database allows the creation of two-dimensional and three-dimensional (elevation) models of any part of the world. NIMA also catalogs man-made and natural features, which can be used for navigational or intelligence purposes.

For information gathering, NIMA uses Department of Defense, NRO, and other government owned imaging satellites. NIMA also contracts out for the use of privately owned imaging satellites in a cost-saving effort. NIMA declassifies many of the images obtained from these commercial satellites for use by American allies.

The National Imagery and Mapping Agency contributes to achieving United States foreign policy and national security objectives by providing intelligence agencies and policymakers with current imagery information. Military and civilian intelligence agencies use NIMA's cartographic and geospatial intelligence to monitor the proliferation of nuclear, chemical, and biological weapons, track arms shipments, and ensure that global treaties are being upheld.

NIMA's primary function is to provide accurate geospatial information for combat planning and support. NIMA tailors its products to fit the needs of its target audience. When the United States began military operations in Afghanistan in 2001, American military forces had little information on Afghan geography and topography. NIMA assisted the various U.S. forces involved in this conflict by quickly producing high quality maps for strategists and soldiers. NIMA used its resources to produce different maps for different operations. Maps for Naval aviators included detailed information about targets for the U.S. bombing campaign. Maps for special operations forces noted possible food and water locations, as well as the locations of enemies and non-combatants.

NIMA provided similar logistical support for Operation Iraqi Freedom in 2003. During the planning stages of the war, NIMA provided policymakers and military coordinators with maps that included the locations of enemy forces, suspected chemical and biological weapons depots, and potential government and military targets. Maps also noted strategic locations, including oil wells. During combat, NIMA's technologically advanced imaging systems supplied U.S. forces with near real-time maps that allowed American forces to engage enemy combatants before visually confirming the enemies' presence.

NIMA is currently working on the Shuttle Radar Topography Mission (SRTM), a mission that recorded elevation data for most of the Earth's surface. By accumulating elevation data from a single source, NIMA will be able to produce a uniform elevation map of the Earth.

#### ■ FURTHER READING:

##### ELECTRONIC:

Department of Defense. "United States National Imagery and Mapping Agency." <<http://www.nima.mil/>> (May 2003).

## SEE ALSO

*Mapping Technology*  
*NASA (National Air and Space Administration)*  
*DOD (United States Department of Defense)*

## NIMH (National Institute of Mental Health)

The National Institute of Mental Health (NIMH) falls under the umbrella of the government's medical research agency, the National Institutes of Health (NIH). The NIMH is the branch of the NIH that focuses on the brain, behavior, and mental health.

The creation of the NIMH in the 1940s ushered in a new approach to the diagnosis and treatment of mental illness. Psychologists began to realize that mentally ill patients would benefit more from evaluation and treatment than from institutionalization, and asylums were gradually replaced by well-equipped, well-staffed mental health facilities. In 1946, President Harry S. Truman signed the National Mental Health Act, which redirected the funding and oversight of mental health programs from the state to the federal level. The act also called for the establishment of the NIMH to lead research efforts relating to the brain and psychiatric disorders. The agency was formally established in 1949.

The NIMH became the foremost behavioral science and mental-illness research center in the country and provided funding and training for state mental health facilities. During the 1960s, the institute expanded its offerings by establishing centers for the study of child mental health, crime, urban mental health issues, and suicide. Alcohol and substance abuse were added as separate areas of study in the late 1960s and early 1970s. Thanks to rapid expansion during the 1960s, the NIMH was separated from the NIH and added to the newly established Health Services and Mental Health Administration, but it rejoined the NIH in 1973.

Scientists at the NIMH use a combination of neuroscience, behavioral science, molecular genetics, and brain imaging to delve into the underlying physiological and genetic mechanisms that trigger mental illness. Their aim is to discover ways to prevent and treat mental illnesses through a combination of pharmacological and behavioral therapies. The agency not only conducts its own laboratory research and clinical trials, but also funds research by universities, private companies, and individual scientists. The NIMH also provides educational materials to patients, medical professionals, local governments, and organizations around the country.

In 2003, the NIMH will conduct a study, following over 200,000 people exposed to the ash and dust resulting from the destruction of the World Trade center by terrorists in 2001. In one of the largest studies ever conducted, the NIMH will observe patterns of illness and recovery among the residents and workers of lower Manhattan. The NIMH also maintains divisions that focus on preparing and coping with disasters and emergencies.

### ■ FURTHER READING:

#### BOOKS:

Mintzer, Richard. *The National Institutes of Health*. Philadelphia, PA: Chelsea House Publishers, 2002.

#### PERIODICALS:

Grob, Gerald N. "Creation of the National Institute of Mental Health." *Public Health Reports* no. 4 (July-August 1996):378-381.

#### ELECTRONIC:

National Institute of Mental Health. <<http://www.nimh.nih.gov/>> (December 7, 2002).

#### SEE ALSO

*NIH (National Institutes of Health)*  
*Public Health Service (PHS), United States*

### 9-11 Terrorist Attacks.

SEE *September 11 Terrorist Attacks on the United States*.

## NIST (National Institute of Standards and Technology), United States

### ■ JUDSON KNIGHT

The National Institute of Standards and Technology (NIST) is a non-regulatory federal agency under the aegis of the Undersecretary for Technology in the U.S. Department of Commerce. It is concerned with maintaining measurement standards and developing technology in order to improve productivity, promote commerce, and enhance the quality of life in the United States. It also has a number of security functions, which have come to the forefront in the aftermath of the September 11, 2001, terrorist attacks upon the United States.

**Background.** Founded in 1901 as the Bureau of Standards, NIST today involves the development and maintenance of standards and measures used in virtually every arena of public and private life. Private industry in the United States uses more than 9,000 NIST standards.

Characterizing the breadth of the NIST mission, Anne C. Mulkern wrote in the *Denver Post*, “When consumers buy beef at the butcher, it’s weighed on a scale that’s calibrated to a NIST-developed standard. Automobile seat belts all must adhere to a safety standard set by NIST.” At its Web site in 2003, the institute itself described the range of areas in which it is involved: “From automated teller machines and atomic clocks to mammograms and semi-conductors, innumerable products and services rely in some way on technology, measurement, and standards provided by [NIST].”

**Organization.** In line with its mission, NIST oversees four major cooperative programs: the NIST Laboratories, which advance the national technology infrastructure; the Baldrige National Quality Program, designed to encourage excellence among U.S. manufacturers, service providers, health-care companies, and educational institutions; the Manufacturing Extension Partnership, a network of local centers that assists small manufacturers; and the Advanced Technology Program, whose function is to promote research and development of new technologies in the private sector.

With a 2003 operating budget of \$810 million, NIST employs some 3,000 scientists, engineers, technicians, and support and administrative personnel. Some 1,600 other guest researchers also work with the institute. Additionally, NIST works with some 2,000 manufacturing specialists and support staff at various locations nationwide. It has two offices: a 578-acre (234-hectare) facility in Gaithersburg, Maryland, and a 208-acre (84-hectare) installation at Boulder, Colorado.

**Intelligence and security work.** In addition to the work of its Computer Security Division and efforts to assist law-enforcement agencies in detecting criminal activity on computers, NIST has played a significant part in the investigation of the September 11 terrorist attacks. Mulkern, writing in January 2002, discussed the greatly enhanced stature of the institute, which at that time was being considered for a lead role in the investigation of the World Trade Center collapse.

NIST scientist Ronald Rehm, according to Mulkern, “goes to work every day and watches the World Trade Center burn, over and over again.” His purpose was not to relive a moment of national agony, but to study it the way a coroner does a cadaver—for clues as to the cause of death. One finding he had already turned up, which contradicted the accepted wisdom about the collapse, was that the temperature inside the buildings was not high

enough to melt steel. Instead, the levels of heat had only been enough to bow the steel, and this alone put enough pressure on the walls and floors that the buildings fell. Additionally, the heat of the jet fuel alone did not explain the rapid spread of the fire, according to Rehm, who had determined that the large paper supplies in the offices, along with other combustible materials, greatly abetted the conflagration.

Not only was NIST involved in the investigation of what happened, it was also deeply concerned with efforts to prevent another such tragedy by helping to interdict suspicious persons. Among its tasks in the post-attack security environment was a mandate from the federal government to develop standards for biometric recognition systems, which use face recognition, retina scanning, voiceprints, and other characteristics of an individual’s physique to provide identification. NIST has also been tasked to study the use of electromagnetic waves as a means of detecting objects hidden under clothing.

#### ■ FURTHER READING:

##### PERIODICALS:

Mulkern, Anne C. “Agency Tackles National Security: NIST’s Boulder Lab Developing Technologies to Combat Terrorism.” *Denver Post*. (January 25, 2002): C1.

Piazza, Peter. “Tools for Digital Sleuths.” *Security Management* 46, no. 4 (April 2002): 36.

##### ELECTRONIC:

National Institute of Standards and Technology. <<http://www.nist.gov/>> (January 28, 2003).

##### SEE ALSO

*Commerce Department Intelligence and Security Responsibilities, United States*  
*IDENT (Automated Biometric Identification System)*  
*NIST Computer Security Division, United States*

---

## NIST Computer Security Division, United States

---

The Computer Security Division (CSD) is one of eight divisions within the Information Technology Laboratory of the National Institute of Standards and Technology (NIST), itself a bureau of the Chamber of Commerce. CSD is concerned with raising awareness of information technology (IT) risks, vulnerabilities, and protection requirements, especially for new and emerging forms of technology.

In addition to its support and security role with regard to new technologies, CSD is involved in researching IT

vulnerabilities, advising federal and state agencies of these, and developing means to provide cost-effective protection. Also, in line with its mission as a part of NIST, it helps develop standards, tests, validation programs, and metrics in computer systems and services with an eye toward security.

NIST involvement in “digital sleuthing,” or the use of computers in detective work, often allows the division to team up with a consortium of law-enforcement agencies to develop computer forensics technology. NIST and CSD scientists worked with agents from the Federal Bureau of Investigation, United States Customs Service, and other agencies, along with software vendors, to create the National Software Reference Library (NSRL), which allows easier review of the contents of a computer, especially with regard to material potentially relevant to a criminal investigation. By examining file tag attachments NIST CSD programs can easily identify certain types of files (e.g., picture files that may be hidden in other programs).

Thanks to Presidential Decision Directive 63, signed by President William J. Clinton in 1998, NIST and CSD received \$5 million (which was much less than the \$50 million Clinton had requested from Congress) to encourage the development of secure information systems for support of the telecommunications, transportation, and government service infrastructures. In the country’s heightened security environment after September 11, the work of CSD has become—like that of most agencies either within or at the periphery of the security and intelligence apparatus of the federal government—critical to national defense. Among the areas of focus for CSD are development of cryptographic standards and applications, security testing, and research in the interests of emerging technologies.

#### ■ FURTHER READING:

##### PERIODICALS:

- Frank, Diane. “NIST Aims Grants at Systems Security.” *Federal Computer Week* 15, no. 11 (April 23, 2001): 12.
- Piazza, Peter. “Tools for Digital Sleuths.” *Security Management* 46, no. 4 (April 2002): 36.
- . “E-mail and Patching Hints from NIST.” *Security Management* 46, no. 7 (July 2002): 44.

##### ELECTRONIC:

- Computer Security Division. National Institute of Standards and Technology. <<http://csrc.nist.gov>> (January 28, 2003).

##### SEE ALSO

- Commerce Department Intelligence and Security Responsibilities, United States*  
*Computer Hardware Security*  
*Computer Software Security*  
*NIST (United States National Institute of Standards and Technology)*

## Nixon Administration (1969–1974), United States National Security Policy

■ CARYN E. NEUMANN

Richard Nixon took office in 1969 as the country struggled to deal with the effects of the war in Vietnam. The inability of the United States to quickly win the war forced a review of national security policy. With the resulting Nixon Doctrine, the U.S. adjusted its foreign commitments to more effectively and efficiently utilize its resources. The Nixon administration pursued an honorable exit in Vietnam, sought peace with the Soviet Union, and reduced tensions with communist China by normalizing relations, while declining to pursue idealistic goals peripheral to the balance of military and geopolitical power.

The Nixon administration began with an overhaul of the national security advisory process. Nixon had apparently harbored resentments over perceived snubs delivered by Foreign Service officers when he served as vice-president under Eisenhower. He also preferred a solitary approach to decision-making. As president, he was determined to circumvent and minimize the State Department’s traditional role in foreign policy in favor of conducting policy from the White House.

The National Security Council (NSC) under Nixon would function as a rival State Department with only adviser Henry Kissinger participating in the President’s important discussions with visiting foreign officials. To further keep the State Department shut out of negotiations with foreign governments, Kissinger relied upon CIA communications for “back channel” messages as he traveled from country to country. The NSC also took control of the process of clearing key policy cables to overseas posts. Secretary of State William P. Rogers, less experienced in foreign affairs, played a minor role in policy formulation. In late 1973, Kissinger replaced Rogers. For the first time, one individual held simultaneously the positions of national security adviser and secretary of state.

The Vietnam War dominated American affairs in the late 1960s and it became the first major dilemma faced by the Nixon administration. To restore American power, Nixon decided to exit Southeast Asia in a way that would preserve the reputation of the U.S. as a country that honored its commitments. The administration elected to pursue a two-pronged approach of a phased withdrawal of ground troops and a modernization of the South Vietnamese military to enable it to assume full responsibility for the fighting. This policy stressed that an allied country must demonstrate the ability to provide for its own security since the U.S. would no longer provide the major defensive effort. The U.S. completed disengagement from Vietnam in 1973.





President Richard M. Nixon (right-center) meets with members of the Security Council on January 21, 1969, his first full day as President of the United States. ©BETTMANN/CORBIS.

While the U.S. had been focused upon Vietnam, the Soviet Union had moved from a position of strategic inferiority to one of strategic parity. The system of mutual deterrence that rested upon the threat of retaliatory annihilation now no longer existed because the Soviets had developed a first-strike capability. Kissinger argued that the Soviets were more likely to be conciliatory if they feared that the U.S. would seek cordial relations with China. Since 1949, when the communists established control on mainland China, the U.S. had preferred to regard the exiled regime on Taiwan as the legitimate Chinese government. However, a Sino-American alliance would create a new balance of power by checking the Soviet superiority in conventional military forces. Accordingly, Nixon visited China in 1972 and drove a wedge between the two chief bastions of communism in the world. The Soviets, now anxious for an easing of tensions (known as *détente*) signed the Strategic Arms Limitation Talks agreement in May 1972 to limit the number of intercontinental ballistic missiles (ICBMs) and the construction of antiballistic missile systems (ABMs).

The Watergate scandal that forced Nixon's resignation in 1974 overshadowed his foreign policy accomplishments and contributed to a perceived mistrust of national leaders. Despite the enormous impact of Watergate, Nixon's pragmatic approach to international relations continues

to influence debates about the proper role of the U.S. in world affairs.

#### ■ FURTHER READING:

##### BOOKS:

- Boll, Michael M. *National Security Planning Roosevelt Through Reagan*. Lexington: University Press of Kentucky, 1988.
- Crabb, Cecil V., and Kevin V. Mulcahy. *American National Security: A Presidential Perspective*. Pacific Grove, CA: Brooks/Cole, 1991.
- Record, Jeffrey. *Making War, Thinking History: Munich, Vietnam, and Presidential Uses of Force from Korea to Kosovo*. Annapolis, MD: Naval Institute Press, 2002.

##### ELECTRONIC:

- White House. "History of the National Security Council, 1947–1997." <<http://www.whitehouse.gov/nsc/history.html>> (April 25, 2003).

##### SEE ALSO

- CIA (United States Central Intelligence Agency)*  
*Cold War (1950–1972)*  
*Cold War (1972–1989): The Collapse of the Soviet Union*  
*Department of State, United States*

*National Security Advisor, United States  
National Security Strategy, United States  
NSC (National Security Council)  
NSC (National Security Council), History*

## NMIC (National Maritime Intelligence Center)

The National Maritime Intelligence Center (NMIC) brings together several military intelligence operations for the United States: Navy, Marine Corps, and Coast Guard. The first of these, being by far the largest, is the dominant participant in NMIC, whose headquarters in Suitland, Maryland, are home to the Office of Naval Intelligence (ONI). NMIC also houses offices for the Naval Information Warfare Activity (NIWA), as well as the principal intelligence agencies of the two smaller services, the Marine Corps Intelligence Activity (MCIA) and Coast Intelligence Coordination Center (ICC).

NMIC does not represent a single command; indeed, it would be hard for it to do so, given the fact that the navy and marines fall under the Department of Defense, while the Coast Guard, as of March 2003, is under the aegis of Department Homeland Security. Rather, NMIC offers a united source for maritime intelligence at the national level, and provides support to joint warfighters of the three services involved, as well as to the Department of Defense (DOD), and to other national agencies and departments requiring maritime intelligence.

The physical facilities of NMIC are located on the 226-acre (91.5-hectare) Suitland Federal Center in Suitland, Prince George's County, Maryland. Situated on the Metro's Green Line alongside the Census Bureau, Washington National Records Center, and Atmospheric Administration, NMIC itself occupies 42 acres (17 hectares). It is housed in a 603,000 square-foot facility (5.6 hectares; depicted on the NMIC Web site, listed below), which contains the headquarters of ONI, as well as offices for NIWA, MCIA, and ICC.

**Historical background.** The origins of NMIC lie in the early 1990s, when the United States, had successfully concluded the Cold War following the fall of the Soviet empire. During this era, long before the war on terrorism that commenced with the attacks on the World Trade Center and Pentagon on September 11, 2001, the federal government began to scale down its defense and intelligence operations.

By September 1991, just after the end of the Cold War, the U.S. Navy had seven intelligence organizations: ONI,

the Naval Intelligence Command (NIC), Task Force 168, the Naval Technical Intelligence Center (NTIC), the Navy Operational Intelligence Center (NOIC), the Naval Intelligence Activity (NIA), and the Naval Security Group Command. Highest in prestige and authority was ONI, with NIC occupying a second level of authority, while all the others—with the exception of the last named—were subordinate to NIC.

In October 1991, the Navy closed down NTIC, Task Force 168, and NOIC. Formerly, Task Force 168 had been involved in overt collection of data from human sources; NTIC had performed the duties of a scientific and technical intelligence organization, specializing in information on the Soviet navy; and NOIC had used signals intelligence to monitor naval forces worldwide. Thenceforth, these offices would fall under a new Naval Maritime Intelligence Center (NAVMIC).

The consolidation continued in January 1993, when the navy disestablished NAVMIC after less than two years, and placed it, along with NIC and NIA, under ONI. The latter would thus take over the functions of the other organizations, including NIA's responsibility for the provision of automatic data processing support to naval intelligence organizations. ONI then was reorganized into eight major directorates, each with direct access to the Director of Naval Intelligence. In 1994, NMIC was formed as a joint operating center for ONI, NIWA, and the intelligence agencies of the marines and Coast Guard.

**Naval components of NMIC.** ONI organizes and trains intelligence personnel; provides highly specialized intelligence analysis related to maritime activities; and operates in an oversight capacity with regard to security and intelligence manpower issues for the navy. It serves as a liaison between DOD and non-DOD agencies, and supports foreign liaisons. Additionally, it is engaged in long-term analysis of foreign military (particularly naval) forces and operations, as well as broader scientific, technical, and strategic trade analysis. ONI is also involved in intelligence systems acquisition.

Established in 1882, ONI has the distinction of being the oldest continually operating intelligence agency in the United States. Until the First World War, it was concerned primarily with collection of technical data on foreign governments and their naval forces, and with conducting war games in association with the Naval War College in Newport, Rhode Island. The world war brought with it expanded responsibilities for ONI, which was deployed to provide security at war material plants, conduct security checks of navy personnel, and hunt down spies and saboteurs.

Just as ONI would survive the downscaling of the U.S. armed forces after the end of the Cold War three-quarters of a century later, it weathered the downsizing of the military that occurred during the interwar period. As Japan began mobilizing for war in the 1930s, ONI, in association with the Navy's Office of Communication,

maintained a close watch on Japanese diplomatic dispatches. After World War II, it endured another period of downsizing, but thanks to the support of Fleet Admiral Chester W. Nimitz, ONI was strengthened rather than reduced in the postwar era.

As of the early twenty-first century, ONI housed the vast majority of its personnel—some 500 military and 1,000 civilians—at NMIC. Even in the aftermath of September 11, it maintained an appearance of relative openness that, while perhaps illusory, served to welcome intelligent and talented men and women as recruits, particularly recruiting architects, engineers, communications analysts, scientists, and mathematicians.

Much more secretive is NIWA, which, while many of its personnel are housed at NMIC, has its headquarters at Fort Meade, Maryland. It serves as the technical agent for the Chief of Naval Operations in pursuit of technologies useful in information warfare. In particular, NIWA is responsible for threat analysis and assessment of vulnerabilities. It evaluates and assesses new forms of information technology, and other concepts relating to naval defensive information warfare systems.

**Marine and Coast Guard components.** MCIA, which also has facilities at Quantico, Virginia, is focused on providing threat assessments and expeditionary intelligence to Marine Corps headquarters. It works with marines in the field, as well as with other services, and with other organizations in the U.S. intelligence community, to provide threat, technical, and terrain analysis tailored to the specific needs of Marine Corps tactical units. It also serves as the primary coordination link with ONI for expeditionary intelligence analysis.

Aside from being much smaller than the “big three”—army, air force, and navy—the Coast Guard and marines could hardly be more different. Whereas the marines are widely perceived as being the most “military” of the military services, the Coast Guard is not even supervised by DOD. And whereas the marines are regularly deployed to far-flung theatres, the Coast Guard’s purview is primarily—though not exclusively—along the U.S. coastline.

Formed in 1984, as the war on drugs began to heat up, ICC included some 50 Coast Guard and civilian personnel as of 2003. Though it is the most notable arm of Coast Guard intelligence, its functions are augmented by intelligence staff who work with the Atlantic and Pacific Coast Guard commanders.

Coast Guard intelligence is concerned with everything from drug smuggling to illegal fishing, and the war on terrorism begun after September 11, 2001, has served to greatly expand its importance as a protector of homeland security. In particular, ICC, and the Coast Guard as a whole, has been tasked with monitoring ships destined for the United States as a means of intercepting terrorist operatives. According to a December 2002 report that appeared in the *Seattle Times*, the al-Qaeda terror network

is assumed to control up to 15 cargo freighters operating under false papers worldwide.

#### ■ FURTHER READING:

##### BOOKS:

Dorwart, Jeffery M. *The Office of Naval Intelligence: The Birth of America’s First Intelligence Agency, 1865–1918*. Annapolis, MD: Naval Institute Press, 1979.

Packard, Wyman H. *A Century of U.S. Naval Intelligence*. Washington, D.C.: Office of Naval Intelligence, 1996.

Richelson, Jeffrey T. *The U.S. Intelligence Community*, 3rd ed. Boulder, CO: Westview Press, 1995.

##### PERIODICALS:

Brinkley, Joel. “Coast Guard Encounters Big Hurdles in New Effort to Screen Arriving Ships.” *New York Times*. (March 16, 2002): A9.

Killian, Michael. “New Defensive Posture for Former Prosecutor: Threat from Sea a Top Priority.” *Chicago Tribune*. (February 13, 2002): 7.

Mintz, John. “Fearing Attack by Sea, U.S. Tracking ‘Ships of Concern.’” *Seattle Times*. (December 31, 2002): A1.

Thompson, Phillip. “A Crystal Ball for Intelligence Needs.” *Sea Power* vol. 44, no. 3 (March 2001): 51–53.

##### ELECTRONIC:

National Maritime Intelligence Center/Office of Naval Intelligence. <<http://www.nmic.navy.mil/nmicpic.htm>> (January 17, 2003).

##### SEE ALSO

*Coast Guard (USCG), United States Homeland Security, United States Department of Information Warfare*

---

## NNSA (United States National Nuclear Security Administration)

---

■ K. LEE LERNER/JUDSON KNIGHT

Created in 1999 and put into operation the following year, the National Nuclear Security Administration (NNSA) was a response to security concerns with regard to United States nuclear materials and information. In order to better protect these sensitive properties, Congress established NNSA as a separate agency within the Department of Energy (DOE). NNSA operates a variety of programs



The Lightweight Epidemiology Advanced Detection and Emergency Response System, better known as LEADERS and demonstrated in this photo, reaches into hospitals and can send fast, automated alerts by scanning electronic records for clues to a bioterror disease outbreak. AP/WIDE WORLD PHOTOS.

geared toward the security of U.S. nuclear stockpiles, while its Nuclear Nonproliferation Verification Research and Development Program works for security in the broader, more global sense. NNSA also has intelligence and incident preparedness responsibilities.

## History

The creation of NNSA was a saga in itself, an outgrowth of concerns over vulnerabilities to Chinese espionage under the administration of President William J. Clinton. Even as political opponents in the Republican Party accused Clinton and Vice-President Al Gore of accepting illegal campaign donations from the Chinese, information surfaced regarding Clinton appointees with close ties to the People's Republic of China. Of most concern were allegations regarding the illegal sale of defense technology to China, as well as evidence of Chinese spying at nuclear labs.

In response to these concerns, Congress in 1999 created NNSA as a "semi-autonomous" agency within DOE. Energy Secretary Bill Richardson, along with other members of DOE leadership, maintained that the new agency would create confusion, obscure the chain of command, and place roadblocks in the way of DOE's environmental and safety oversight roles. Nevertheless,

Clinton signed the legislation, which had been linked to defense appropriations for 2000.

Clinton then authorized Richardson "to perform all duties and responsibilities" of the newly created Undersecretary of Energy for Nuclear Security position, the director of NNSA. In so doing, he effectively circumvented the congressional attempt to pull nuclear materials from direct DOE authority, a move that infuriated congressional Republicans.

Under the threat that Congress would cut the pay of top DOE officials, Richardson met with House leaders. After some discussion, the White House put forward former Air Force General John Gordon, then serving as deputy director of the Central Intelligence Agency (CIA), as the first NNSA director and undersecretary for nuclear security.

## Mission and Organization

NNSA, which began operation on March 1, 2000, has the mission of improving national security through defense uses of nuclear energy; maintaining the U.S. nuclear stockpile, and enhancing its safety, reliability, and performance; providing the U.S. Navy with safe, reliable, and effective nuclear propulsion plants; advancing nuclear

safety and nonproliferation internationally; reducing the global threat posed by weapons of mass destruction; and supporting America's leading role in the realms of science and technology.

The NNSA administrator oversees all functions of NNSA except those accorded to the deputy administrator for naval reactors by Executive Order 12344 (Naval Nuclear Propulsion, February 1, 1982). The administrator's responsibilities include strategic management, policy development and guidance, program management and direction, budgets and other financial matters, resource allocation, safeguards and security, emergency management, environment and health matters, administration of contracts, intelligence, counterintelligence, personnel, procurement, legal matters, legislative affairs, public affairs, and interactions with other DOE offices and other units of federal, state, and local government.

NNSA staff supports the administrator in a number of these functions, particularly counterintelligence, nuclear security, legal affairs, policy planning and assessment, legislative and intergovernmental affairs, public affairs, and matters of the environment, safety, and health. Also reporting to the administrator are deputy administrators for defense programs, nonproliferation, and naval reactors. There are also associate administrators for facilities and operations, and for management and administration.

At the heart of NNSA is the Nonproliferation Verification Research and Development Program, which operates, or has operated, a number of programs. Among these is the International Materials Protection, Control, and Accounting Program, whereby NNSA personnel work with Russia and former Soviet republics to ensure against proliferation, to return to the country of origin all weapons-usable nuclear materials, to convert or dispose of those materials wherever possible, and to develop new safeguards.

The Nonproliferation Verification Research and Development Program is responsible for creating and testing detection systems that will advance America's ability to respond to national threats from nuclear, chemical, or biological weapons. Its three principal elements are the monitoring of nuclear explosions and tests, a function overseen by DOE; proliferation detection; and the Chemical and Biological National Security Program (CBNP).

**Nuclear smuggling and threat assessment.** As explained by Linton F. Brooks, NNSA administrator under President George W. Bush, in a statement to the House of Representatives Energy and Commerce Committee on July 9, 2002, the technologies developed in the proliferation detection segment serve functions both of nonproliferation and homeland security. Accordingly, those areas supportive of homeland security that could be separated from NNSA would move to the new Department of Homeland Security (DHS).

Among the key components of the proliferation detection program is the nuclear smuggling component. In this area, NNSA, together with the U.S. National Laboratories, put to use unique insights regarding nuclear proliferation, including the characteristics or "signatures" of particular weapons. Working with such future DHS agencies as U.S. Customs and the U.S. Coast Guard, as well as the departments of Transportation and Justice, NNSA had conducted demonstrations of radiation detection methods at international ports, border rail yards, and airports.

Also scheduled for transfer was the DOE Nuclear Threat Assessment Program. Initiated at Lawrence Livermore National Laboratory in September 1978, the program had been applied in assessing the credibility of more than 60 threats of nuclear extortion, 25 claimed threats to nuclear reactors, 20 non-nuclear extortion threats, and some 650 instances involving the attempted or alleged sale of nuclear materials. As nuclear threats are a federal violation, credibility assessment teams work under Federal Bureau of Investigation direction, in conjunction with representatives of CIA, the Defense Intelligence Agency, Customs, and the State Department. In the aftermath of the September 11, 2001, terrorist attacks, one of the key tasks of the program was the separation of critical from non-critical information as to possible threats.

**CBNP.** Also moved to DHS was CBNP. CBNP actually predates NNSA, having been initiated by DOE in 1997 to respond to events such as the Tokyo nerve-gas attack that took place two years earlier. The program develops systems and technologies to protect civilian populations against the threats of the modern battlefield. NNSA and the national laboratories of DOE have undertaken extensive studies in chemistry, biology, materials science, and engineering to develop prototypes, which, if approved, can actually be manufactured by outside bidders.

For example, CBNP, in conjunction with the Centers for Disease Control, conducted research on the biological foundations required to establish signatures of biological agents—that is, DNA profiles of pathogens, such that medical personnel would be able to more quickly treat victims. These signatures would also provide forensic evidence for the prosecution of terrorists. One practical creation of this program may be a palm-sized device, identified by a CBNP project manager in early 2001 as the Chemlab, that will be able to detect and identify biological agents quickly and accurately.

To maintain cost effectiveness, CBNP attempts to use existing technology as much as possible. For example, one area of research is in microchips or cards that could plug into existing palm-size computers to detect dangers ranging from toxins to viruses. CBNP also adapted existing technology for its RSVP, or Rapid Syndrome Validation Program, a software package that makes it possible for doctors to network regarding the symptoms they see in patients—a highly useful tool in the event of a biological attack.

CBNP also conducts or directs exercises, such as the PROTECT subway demonstration, designed to simulate the 1995 Tokyo attacks. In the Nevada desert, at a site where nuclear tests were once conducted, NNSA operates the Weapons of Mass Destruction Terrorism Response Domestic Preparedness Program, a counterterrorism training facility. Up to 100 personnel from law-enforcement and emergency-response departments around the country train there, undergoing rigorous simulations that may involve being woken at 2:00 a.m. with cries of "Terrorists have taken hostages at a nuclear facility!" Among those trained at the site prior to September 11, 2001, were New York City law enforcement personnel who later put their training to use in an all too vivid real-life experience.

#### ■ FURTHER READING:

##### BOOKS:

*Homeland Security: Hearing Before the Committee on Energy and Natural Resources, United States Senate, One Hundred Seventh Congress, Second Session on the Present and Future Roles of the Department of Energy/National Nuclear Security Administration National Laboratories in Protecting Our Homeland Security, July 10, 2002.* Washington, D.C.: U.S. Government Printing Office, 2002.

*National Nuclear Security Administration: Joint Hearing Before the Committee on Energy and Natural Resources and the Committee on Governmental Affairs, United States Senate, One Hundred Sixth Congress, First Session on the Department of Energy's Implementation of Provisions of the Department of Defense Authorization Act Which Create the National Nuclear Security Administration, October 19, 1999.* Washington, D.C.: U.S. Government Printing Office, 2000.

*Safety and Security Oversight of the New National Nuclear Security Administration: Joint Hearing Before the Subcommittee on Energy and Power and the Subcommittee on Oversight and Investigations of the Committee on Commerce, House of Representatives, One Hundred Sixth Congress, Second Session, March 14, 2000.* Washington, D.C.: U.S. Government Printing Office, 2000.

*The Secretary of Energy's Priorities and Plans for Department of Energy National Security Programs: Hearing Before the Committee on Armed Services, United States Senate, One Hundred Seventh Congress, First Session, February 8, 2001.* Washington, D.C.: U.S. Government Printing Office, 2002.

##### PERIODICALS:

Bleek, Philipp C. "New DOE Nuclear Security Organization Begins Work." *Arms Control Today* 30, no. 3 (April 2000): 29–30.

Dao, James. "Nuclear Study Raises Fears About Weapon." *New York Times*. (November 17, 2002): section 1, p. 22.

Gorman, Tom. "Rescue Worker Boot Camp." *Los Angeles Times*. (October 11, 2001): A6.

Johnson, Jeff. "Unclear Future at Weapons Labs." *Chemical & Engineering News* 78, no. 49 (December 4, 2000): 51–58.

Pincus, Walter. "DOE Plan Riles Senate GOP: Choice of Richardson to Run New Bomb Agency Spurs Pay Threat." *Washington Post*. (October 19, 1999): A17.

———. "Nuclear Security Gets First Director: Gordon Confirmed as GOP Blasts His Boss, Richardson." *Washington Post*. (June 15, 2000): A31.

Warchol, Glen. "Beam Us Up, Scotty: 'Tricorder' May Fight Biological Threats." *Salt Lake Tribune*. (May 7, 2001): D1.

##### ELECTRONIC:

National Nuclear Security Administration. <<http://www.nnsa.doe.gov>> (March 7, 2003).

##### SEE ALSO

*Chinese Espionage Against the United States DOE (United States Department of Energy) Nonproliferation and National Security, United States Nuclear Weapons*

---

## NOAA (National Oceanic & Atmospheric Administration)

---

The National Oceanic & Atmospheric Administration (NOAA) monitors environmental, climatic, and weather conditions in the United States and around the world. The administration manages an extensive network of satellites, sensory aircraft, and specialized monitoring equipment to provide information on meteorological events and their impact. The mission of NOAA is to protect persons, property, national security, and United States economic interests. NOAA also works with foreign meteorological services, international search and rescue units, and independent research scientists.

The administration has several operating divisions responsible for various agency responsibilities and research programs. The National Weather Service (NWS) is perhaps the most well known NOAA operational division. The NWS maintains the most extensive satellite network and meteorological research equipment, providing national, regional, and local weather through a variety of media. NOAA Weather Radio, the voice of the National Weather Service, broadcasts constant weather updates and is linked to the Federal Emergency Management Agency's Emergency Broadcast System. Though developed for government use, the radio broadcasts are available to private citizens.

In conjunction with the Department of Defense, NOAA also oversees the Defense Meteorological Satellite Program (DMSP). A key component of aerospace development, the space program, and weapons development, the

DMSF organizes the construction, launch, and maintenance of satellites that monitor atmospheric, oceanographic, and solar-terrestrial environments. The DMSF maintains a large network of satellites 1330 miles (about 850 km) above the earth's surface. Data from the satellites is sent to the Air Force Weather Agency, the National Geophysical Data Center, and the National Center for Atmospheric Research.

Another NOAA division, the National Environmental Satellite, Data, and Information Service (NEDIS) provides information on significant environmental events recovered from satellite imagery and other means of remote sensing. The NEDIS also licenses commercial remote sensing satellites, including global positioning systems (GPS). In conjunction with Russia's Cospas satellite system, the NOAA Cospas-Sarsat system can locate lost or endangered individuals through emergency transmissions. NOAA Geostationary Operational Environmental Satellites (GOES) detect signals from Emergency Position Indicating Radio Beacons on boats, airplanes, and other individual vessels, and send information to search and rescue teams. In 2002, nearly 1,500 people were rescued worldwide, most of them at sea.

NOAA's charting and marine safety programs provide information, products, and services that aid marine traffic, commerce, and private use of domestic and international waterways. NOAA creates and distributes tidal and current tables, conducts hydrographic surveys, works closely with several other government agencies to constantly update marine and terrestrial charts and maps. Recently, NOAA began testing International Electronic Navigational Charts, or "smart charts" for private civilian use. Smart Charts work in conjunction with global positioning systems and weather satellites to aid safe navigation. NOAA also develops aeronautical charts used by government and commercial airplanes.

Aside from its role in security, NOAA also funds and conducts research on the global environment and ocean systems. Via satellite and other sensor mechanisms, the administration monitors conditions such as widespread deforestation, ozone depletion, volcanoes, fires, and water pollution. Special attention is paid to the long-term effects of these processes on atmospheric and marine systems and their potential impact on global environments, flora and fauna, climate, and economic systems.

#### ■ FURTHER READING :

##### ELECTRONIC:

United States National Oceanic & Atmospheric Administration. <<http://www.noaa.gov>> (15 January 2003).

##### SEE ALSO

*Coast Guard (USCG), United States*  
*FEMA (United States Federal Emergency Management Agency)*  
*Remote Sensing*

## Noise Generators

■ DAVID TULLOCH

Generating noise is a simple, cheap, and versatile method of blocking signals or shielding communication from a range of devices. From the disruption of radio broadcasts to the masking of conversations, noise generators use a simple concept to great effect.

Noise is an unpredictable disturbance that causes errors in the transmission of all types of communication. Background chatter at a party, static on a radio, poor handwriting, a patchy cellphone connection, and 'snow' (electronic interference) on a television screen are all examples of noise.

By flooding a frequency, or band of frequencies, with noise, the original communication signal can be drowned in a sea of static. Noise generation has been used to jam torpedo guidance systems and block battlefield communications. During the Cold War the broadcasts of Radio Free Europe and the Voice of America were often jammed by Soviets using a network of radio transmitters that covered the entire Soviet Union. In the 1970s the British government jammed pirate radio stations in an attempt to maintain control of the airwaves.

However, by far the most widespread use of noise generators is as a countermeasure against listening devices. The monitoring of conversations is not an activity limited to the world of spies. Companies and individuals are often bugged by rivals seeking to gain private information, and government agencies often spy on the activities of suspected individuals, illegal or otherwise. While removing potential bugs is the surest way to avoid being overheard sometimes this is not possible, or there are doubts that all the listening devices have been detected. Acoustic noise generators can stop the monitoring of spoken conversations from microphone and tape recorders, transmitting bugs, carrier current transmitters, through-wall devices, laser bounce listening equipment, and infrared transmitters. Because they can protect against such a wide variety of covert devices, and do not require the bugs to be found, acoustic noise generators are versatile and popular security items.

#### ■ FURTHER READING :

##### BOOKS:

Johnson, William, with Jack Maguire. *Who's Stealing your Business?: How to Identify and Prevent Business Espionage*. New York, NY: AMACOM, American Management Association, 1998.

Petersen, Julie K., *Understanding Surveillance Technologies: Spy Devices, their Origins & Applications*. Boca Raton, FL : CRC Press, 2001.

## SEE ALSO

*Bugs (microphones) and Bug Detectors*  
*Laser Listening Devices*  
*Microphones*

## Nongovernmental Global Intelligence and Security

Global intelligence and security is not purely the province of governmental agencies. An important advisory role is occupied by think tanks, private corporations, university departments, and other groups. Some of these pursue specific ideological or policy goals, while others are avowedly neutral. Some have specific points of focus, for example on weapons or economic issues. Most are not-for-profit, but not all: an important sector of analysis on global intelligence and security involves companies ranging from publishers to insurers.

**Governmental and nongovernmental groups compared.** In the realm of global security and intelligence, the most visible roles belong to national agencies, particularly those of the world's one superpower, the United States. Also significant are groups such as Interpol and the Financial Action Task Force on Money Laundering, which oversee intelligence and security across national lines.

There are also the military and action forces of international organizations such as the North Atlantic Treaty Alliance (NATO) or the United Nations (U.N.): though neither has its own army, under certain circumstances national armies serve these international organizations. NATO, the U.N., and other groups also have their own policy, oversight, and executive teams that play significant roles, a notable example being the U.N. weapons inspection teams active in Iraq since 1991.

In addition to these agencies and instruments of national governments and multinational quasi-governmental entities, there are also civilian groups that serve in advisory, analysis, and sometimes even action roles. They lack the power to make or enforce laws, of course, but their recommendations are often of value to governments, which in many cases regularly call on their expertise. Included in this broad array of entities are university departments and schools, think tanks and research foundations, study centers, independent evaluation firms, information providers, risk management companies, and others.

**Think tanks.** The range of groups that provide research, analysis, and policy recommendations to governmental bodies is enormous. A leading example is RAND, a name

formed from the contraction of "research and development." Though it is independent, RAND was created in 1946 by the Army Air Forces to evaluate aircraft and other technology. Since that time, RAND's staff has grown to include more than 1,600 persons, most of them involved in research across a variety of disciplines that include not only defense and technology but also public policy.

Another important analysis group is the Center for Strategic and International Studies (CSIS), which at different times has involved such leading public figures as former Senate Armed Services Committee chairman Sam Nunn, former Defense Secretary John J. Hamre, and former National Security Adviser Brent Scowcroft. The mission of CSIS is to advise world leaders on current and emerging global issues by providing strategic insights and policy solutions.

**Across the ideological spectrum.** RAND and CSIS are both examples of "think tanks," or multidisciplinary research institutions. One of the nation's first think tanks was the Hoover Institution, founded in 1919 by future United States President Herbert Hoover. Its original purpose was to study the causes of World War I, but by the beginning of the twenty-first century it had grown to include more than 60 scholars specializing in areas ranging from international relations to economics. During the cold war, the Hoover Institution's annual reports on communist movements worldwide were a key information source for U.S. policy analysts.

Many think tanks have a particular ideological agenda. For example, on the political right, in addition to the Hoover Institution, there is the Heritage Foundation, whose recommendations typically favor reduction of government spending in most areas other than defense. On the political left, by contrast, is the Brookings Institution, which is dedicated to a model of government as an instrument of their visions of national and international social justice, as well as the Carter Center, established by former President James E. Carter. On the other hand, there are numerous academic policy research groups, departments, and schools—several notable examples are affiliated with Georgetown University in Washington, D.C.—that have no obvious or overt political leaning.

**Profit-making enterprises.** While most entities involved in global security and intelligence are nonprofit organizations, this is not true of all. One of the most respected sources of information on military equipment of all types, as well as other kinds of security- and intelligence-related information, is the English-based publisher Jane's. A childhood fascination with warships on the part of its founder, Fred T. Jane, led to the publication of the first edition of *Jane's All the World's Fighting Ships* in 1898. By the beginning of the twenty-first century, Jane's published about 200 different products, including *Jane's Defence Weekly*, *Jane's Fighting Ships*, and *Jane's All the World's Aircraft*.



Other examples of for-profit businesses involved in world security and intelligence analysis include companies in the insurance industry and the related field of risk management. In order to calculate the costs of insuring persons and properties in various locales, it is necessary for companies to possess detailed information on the security climate, including threats related to government coups, asset seizure, and terrorist attack. Some insurers may even employ the services of private hostage-rescue companies that effectively function as non-governmental special-operations teams.

#### ■ FURTHER READING:

##### ELECTRONIC:

Brookings Institution. <<http://www.brookings.edu>> (February 27, 2003).

Center for Strategic and International Studies. <<http://www.csis.org>> (February 27, 2003).

Heritage Foundation. <<http://www.heritage.org>> (February 27, 2003).

Hoover Institution. <<http://www-hoover.stanford.edu>> (February 27, 2003).

Jane's. <<http://www.janes.com>> (February 27, 2003).

RAND. <<http://www.rand.org>> (February 27, 2003).

##### SEE ALSO

*Interpol (International Criminal Police Organization)*

## Nonlethal Devices.

SEE *Less lethal Weapons Technology.*

# Nonproliferation and National Security, United States

The United States government has long had an interest in nonproliferation as a means of ensuring national security. The logic governing this interest is straightforward: as long as weapons continue to proliferate among foreign and hostile powers, U.S. national security remains under threat. At the same time, weapons buildups in other nations arguably necessitate a corresponding buildup in the United States. This can have a number of undesirable effects, ranging from increased spending to a heightened chance of a confrontation such as the one that occurred during the Cuban Missile Crisis of October 1962.

U.S. interest in nuclear nonproliferation dates to the 1950s, when the United States ceased to be the sole

atomic power, and the Soviet challenge greatly increased the chances of global nuclear war. In 1968, the United States, Soviet Union, and United Kingdom made explicit their desire for limits on proliferation through the Nuclear-Non Proliferation Treaty. This was one of several key turning points in the Cold War, as the United States and Soviet Union for the first time began to establish specific limits on nuclear arsenals and the buildup of weapons. These treaties and talks, which began in the late 1960s and continued in various forms for two decades, served to change the character of the Cold War, greatly reducing the threat of open superpower confrontation and limiting the battle to relatively low-level conflicts.

Since 1992, after the end of the Cold War, the United States has devoted considerable effort to overseeing the destruction of nuclear weapons in the former Soviet Union, and to preventing the proliferation of nuclear, biological, or chemical weapons among other nations such as North Korea, Iran, and Iraq. To this end, President William J. Clinton in September, 1998, created the position of Assistant Secretary of Energy for Nonproliferation and Nuclear Security. Two years later, the newly created National Nuclear Security Administration, a unit of the Energy Department, took over these responsibilities. Additionally, the State Department has its Bureau of Arms Control, established in 1999, while the Director of Central Intelligence (DCI) oversees the DCI Center for Weapons Intelligence, Nonproliferation, and Arms Control.

#### ■ FURTHER READING:

##### PERIODICALS:

Gallucci, Robert L. "Non-Proliferation and National Security." *Arms Control Today* 24, no. 3 (April 1994): 13.

Pincus, Walter. "U.S. Agrees to Funds for Russian Scientists." *Washington Post*. (September 20, 1998): A26.

##### ELECTRONIC:

Carnegie Endowment for International Peace. <<http://www.ceip.org/>> (April 5, 2003).

National Nuclear Security Administration. <<http://www.nn.doe.gov/>> (April 5, 2003).

Nuclear Non-Proliferation, 1945–1990. George Washington University. <<http://www.gwu.edu/~nsarchiv/nsa/publications/nnp/nuclear.html>> (April 5, 2003).

##### SEE ALSO

*Arms Control, United States Bureau  
Cold War (1972–1989): The Collapse of the Soviet Union  
Cuban Missile Crisis  
DCI (Director of the Central Intelligence Agency)  
International Atomic Energy Agency (IAEA)  
Iraq War: Prelude to War (The International Debate Over the Use and Effectiveness of Weapons Inspections.)  
NNSA (United States National Nuclear Security Administration)  
North Korean Nuclear Weapons Programs  
Nuclear Weapons  
START I Treaty*

**START II**  
*Strategic Defense Initiative and National Missile Defense Weapons of Mass Destruction*

**NORAD**

■ CARYN E. NEUMANN

The North American Air Defense Agreement, signed on May 12, 1958 by the United States and Canada, created a continental air defense warning and surveillance system in response to Cold War fears of an airborne attack by the Soviet Union. The resulting North American Air/Aerospace Defense Command (NORAD) has since shifted strategies from guarding against long-range bombers to warning of ballistic missile attacks and maintaining space surveillance. While both North American countries provide considerable support for NORAD, the United States, as the dominant partner, makes major policy and leadership decisions.

During the 1950s, the United States aimed to deter any attacks by the Soviet Union on North American soil by

threatening massive retaliation. The main Soviet menace in this era came in the form of long-range bombers that would likely fly over Canadian territory to reach American targets. Because any Soviet attack upon the U.S. would involve Canada, it was logical for the U.S. to form an official military alliance with its neighbor to the north. NORAD formalized a cooperative air defense agreement that had existed between the Royal Canadian Air Force and the U.S. Air Force (USAF). It brought the two nations together to develop continental air defense plans; to maintain and operate the land-based radar and communications systems that would warn of an impending attack; and, in the event of an attack, to employ air defense forces to direct a retaliatory strike away from heavily populated areas. In light of the population density of the U.S., the agreement meant that Canada consented to direct any conflict towards its sparsely peopled north.

Although NORAD is a joint military command, Canada is clearly the subordinate partner. The agreement provides for an American Commander-in-Chief (CINCNORAD) and a Canadian Deputy Commander headquartered in the U.S., at Peterson Air Force Base in Colorado Springs, Colorado. Military and civilian personnel from both countries are assigned to all NORAD elements, but the pilots assigned to intercept threats generally come from the ranks of the USAF. North America is divided into



Large computer screens display maps of the globe inside the main command center for the North American Air/Aerospace Defense Command (NORAD) in Cheyenne Mountain Air Station, 1997. AP/WIDE WORLD PHOTOS.



The “steel city” defense complex of the North American Air/Aerospace Defense Command, NORAD, shown in 1997, was carved out of Cheyenne Mountain in Colorado in the early 1960s. Fifteen steel buildings inside the mountain stand on rows of huge steel springs, designed to negate the earthquake effect of a nuclear blast. AP/WIDE WORLD PHOTOS.

three regions per the NORAD agreement: Alaska, Canada, and the continental U.S., and each of these regions receives information from a surveillance network of ground-based radars augmented by airborne radars, such as those carried by spy planes like the SR-71 and satellites. Federal Air Administration (U.S.) and Transport Canada radars also feed into the network.

In the 1960s, the nuclear-tipped intercontinental ballistic missile and the race for dominance in space began to dominate defense concerns and the emphasis of NORAD was adjusted to respond to these new concerns. The 1966 renewal of the NORAD agreement gave the command responsibility for North American aerospace attack warning and control. Aerospace warning involves the monitoring of man-made objects in space as well as the detection, assessment, and warning of any threat against North America whether by aircraft, missiles, or man-made space vehicles. Aerospace control includes the duties of providing surveillance and control of Canadian and American airspace. In 1974, NORAD began providing surveillance,

warning, and assessment services to command authorities stationed worldwide to assist in deterring attacks upon North American soil.

When the Cold War came to a close in 1989, NORAD struggled to find a role in the absence of an organized military threat. It joined the American War on Drugs in 1989 when Congress requested that the USAF interdict smugglers. Military authorities gave the anti-smuggling duties to NORAD because of its intelligence systems. NORAD received official responsibility for fighting drug trafficking in 1991 and joined the war against terrorism in 1996 when it received a mandate to identify and eliminate a limited missile attack, such as a terrorist launch, an accidental launch, or a launch by a Third World nation.

Despite these activities, NORAD activity began to wind down in the mid-1990s. The Over-the-Horizon Backscatter (OTH-B) radars in the U.S. were shut down. The North Warning System was operating at about 50% of its capacity and needed about three months to be brought back to full activation. The thirty interceptor bases were

reduced to thirteen, with pilots now on a one-hour recall instead of a five-minute callback. A Cold War-era concept, NORAD served its purpose and now its mission in the twenty-first century remains uncertain.

#### ■ FURTHER READING:

##### BOOKS:

Crosby, Ann Denholm. *Dilemmas in Defence Decision-Making: Constructing Canada's Role in NORAD, 1958–96*. New York: St. Martin's Press, 1998.

Lindsey, George R. *The Strategic Defence of North America*. Toronto: The Canadian Institute of Strategic Studies 1986.

Murray, Douglas. "NORAD and U.S. Nuclear Operations," in *Fifty Years of Canada-United States Defense Cooperation: The Road from Ogdensburg*. Edited by Joel J. Sokolsky and Joseph T. Jockel. Lewiston, Maine: Edwin Mellen, 1992.

North American Aerospace Defense Command. *NORAD: Into the 21st Century*. Colorado Springs, Colorado, 1997.

##### SEE ALSO

*Aviation Intelligence, History*  
*Ballistic Missiles*

*Cold War (1950–1972)*

*Cold War (1972–1989): The Collapse of the Soviet Union*  
*RADAR*

*SR-71 Blackbird*

*Terrorism, Intelligence based Threat and Risk Assessments*

## North Korea, Intelligence and Security

The nation of North Korea was established on September 9, 1948, during the grab for satellite nations at the beginning of the Cold War. Supported by the Soviet Union, North Korea established a communist regime under dictator Kim Il-sung. The new government gained popularity by nationalizing former Japanese-owned and remnant European colonial industries and economic interests. Cold War politics plunged the region into war between 1950 and 1953. After the Korean War, North Korea distanced itself from the Soviet Union and became more reactionary and isolationist.

North Korea continues to resist reforms, and relies on the cult of personality of its leaders, and an oppressive political espionage and censorship system, to preserve the nation's communist regime. The North Korean intelligence committee is largely a political mechanism, conducting domestic and foreign political espionage. In recent years, North Korea has taken increasing interest in gathering foreign intelligence on weapons and nuclear systems.

The Cabinet General Intelligence Bureau is North Korea's main intelligence and security agency. Concentrating on foreign intelligence, the agency's Liaison Department actively seeks to subvert the governments of Japan and South Korea, and conducts espionage on United States interests in those nations. The Research Department for External Intelligence (RDEI) collects and analyzes all foreign intelligence gathered by North Korean agents and remote listening equipment. The agency shares information with the communist Central Committee and North Korean leaders.

Preservation of internal security is the main mission of the Ministry of Public Security and the State Security Department. However, in North Korea, internal security is defined in wholly political terms. The ruling political party, the Korean Worker's Party, controls the agencies' network of informants and most resources of the intelligence community. The director of the State Security Department was ousted in 1987, and the directorship was likely assumed by North Korean leader, Kim Jong-il. The State Security Department regularly engages in political espionage, surveillance of citizens and government officials, and monitoring of communication systems. The agency also contributes to the pervasive censorship of all means of expression, such as media and personal speech.

In 2003, North Korea reactivated a nuclear reactor earlier ordered closed under international nuclear non-proliferation agreements. North Korea also announced plans to construct a complex for processing nuclear materials. The international community suspects North Korea of possessing weapons of mass destruction, including intercontinental ballistic missile capability. The region remains a geo-political hot spot, despite efforts of the international diplomatic community to disarm North Korea.

#### ■ FURTHER READING:

##### ELECTRONIC:

Global Security.org. North Korean Intelligence Agencies. <<http://www.globalsecurity.org/intell/world/dprk/>> (March 26, 2003).

##### SEE ALSO

*Korean War*

*Non-Proliferation and National Security, United States*  
*North Korean Nuclear Weapons Programs*

## North Korean Nuclear Weapons Programs

#### ■ K. LEE LERNER

In October 2002, North Korean officials announced that, in violation of an agreement with the United States, North

Korea had a secret program to “enrich uranium for nuclear weapons.”

**History.** With the assistance of the Soviet Union, the Democratic People’s Republic of Korea (DPRK, also known as North Korea) constructed a nuclear complex at Yongbyon in the 1960s. In the late 1970s, North Korea expanded these facilities to include an operational 5 MW natural uranium, graphite-moderated reactor. North Korea also constructed an ore processing plant and a fuel rod fabrication plant.

In 1977, North Korea agreed to IAEA mentoring of its Soviet-supplied 2MW research reactor and 0.1MW critical assembly facility located at Yongbyon. In 1985, the DPRK signed the Treaty on the Non-Proliferation of Nuclear Weapons (NPT). Shortly thereafter, however, North Korea started construction on two gas-graphite reactors in Yongbyon and also started the construction of radiochemical and reprocessing facilities. United States intelligence suspected North Korea was attempting to develop a nuclear weapons program.

In 1990, before the fall of the Soviet Union, the Soviet government announced a halt to the exportation of nuclear equipment and fuel to North Korea. North Korea continues to refuse to sign IAEA inspection agreements until “the United States removes nuclear weapons from South Korea.” The United States rejects North Korea’s demand, in part because of North Korea’s larger conventional forces on the Peninsula. The North Korean statement began a series of shifting demands (including demanding a promise from the United States that it never attack North Korea) as preconditions to cooperation. North Korean President Kim Il-sung continually declined attempts at a diplomatic solution to the impasse.

In 1991, South Korean Defense Minister Lee Jong-ku announced that South Korea might use military force to destroy North Korea’s nuclear facilities at Yongbyon if North Korea does not agree to inspections and IAEA safeguards. North Korean President Kim Il-sung terms the statement a “virtual declaration of war” but continued to decline attempts at a diplomatic solution to the impasse.

Then International Atomic Energy Agency (IAEA) director, Hans Blix, asked the United Nations Security Council to seek more aggressive inspections of facilities in countries suspected of violating the NPT. North Korea declared United Nations efforts a hostile act but began talks aimed at eventually allowing more detailed inspections. North Korean defector, Ko Young-hwan, subsequently revealed that North Korean leaders never intended to commit to rigorous international inspections and that North Korean diplomatic efforts were aimed at securing a place in the United Nations and to allow North Korean nuclear weapons programs time to advance.

In 1992, under threat of possible United States action, North Korea agreed to an IAEA-monitored NPT Safeguards Agreement. IAEA monitoring and inspections start soon after the U.S. informed North Korea that it would

impose sanctions if North Korea does not permit full international inspections of its nuclear facilities.

At the outset of inspections, North Korea admitted in a report to the IAEA and United Nations to having “nuclear material and design information, a fuel rod fabrication plant and storage facility at Yongbyon, a research reactor and critical assembly at the Institute of Nuclear Physics, a sub-critical facility at Kim Il-sung University in Pyongyang, two uranium mines and two centers for uranium concentrate production, a 5 MW nuclear reactor and a radiochemical laboratory under construction at the Institute of Radiochemistry in Yongbyon, a 50 MW nuclear plant under construction in Yongbyon, a 200 MW plant under construction in Taechon, and three planned 635 MW nuclear reactors.” North Korea declared that its radiochemical laboratory was intended for uranium separation research and for plutonium waste management. North Korea also announced its intentions to continue nuclear development, including research on a potential fast-breeder reactor, the development of composite nuclear fuel, and completion of the reprocessing facility at Yongbyon.

Once inspections started, IAEA inspectors found discrepancies between the status of DPRK nuclear programs and DPRK claims in its formal declarations to the IAEA. After comparing physical inspection reports with DPRK declarations, IAEA inspectors suspected that North Korea might possess undeclared plutonium stores. North Korean officials refused IAEA requests to conduct additional inspections to clarify the situation. Inspectors were also specifically blocked from inspecting sites that the North Koreans denied existed but which were known to IAEA inspectors because of intelligence (including spy satellite photographs) supplied by the United States. North Korean representatives subsequently claimed the photographs—although derived from multiple imaging locations—were fake.

Despite claims of having nothing to hide, North Korea threatened to withdraw from the NPT if IAEA inspectors continued to demand to inspect suspect facilities shown in United States intelligence photographs.

Special requests for inspections continued to be rejected by North Korea and in April 1993, the IAEA ruled that North Korea was in “non-compliance” with its agreements regarding nuclear inspection and safeguards. The United Nations Security Council insisted that North Korea comply with its prior agreements. As a result, North Korea announced that it would withdraw from the Treaty on the Non-Proliferation of Nuclear Weapons. After two months of tense diplomatic negotiations, in June 1993 North Korea announced that it had “suspended the effectuation” of its withdrawal from the NPT.

**The framework agreement.** Limited inspections of North Korean nuclear facilities took place for the remainder of 1993 and into 1994. During that time IAEA inspectors concluded that their limited inspections could not provide

“meaningful assurance” that North Korea was using its nuclear facilities for peaceful purposes (e.g., only for energy generation or authorized research). United States President William Jefferson Clinton stated that North Korea’s offer to allow IAEA inspectors access to a portion of its nuclear sites was “inadequate and unacceptable.” In March 1994, North Korea ignored another call by the U.N. Security Council to allow more complete and comprehensive inspections of their nuclear program.

In the summer of 1994, North Korean scientists discharged the fuel from their operational 5 MW reactor. This action effectively prevented IAEA inspectors from employing testing procedures that could have verified North Korea’s declared use of the reactor core or whether nuclear materials had ever been diverted from the core. Soon thereafter, North Korea withdrew from its agreements and membership with IAEA. In accord with prior agreements, neither the IAEA or United Nations considered North Korea released from its treaty and safeguard agreements.

To break the impasse, the United States started direct negotiations with North Korea and entered into a Framework Agreement in October 1994. Under the Agreed Framework the United States pledged to provide fuel for electrical generation and aid in the construction of limited use reactors in exchange for a North Korean freeze and eventual dismantlement of reactors capable of producing weapons grade materials (e.g., graphite-moderated reactors and related facilities). As a consequence of the agreement, the Korean Peninsula Energy Development Organization (KEDO) was formed to facilitate fuel shipments to North Korea.

An important and direct consequence of the agreed framework between the United States and North Korea was the return of IAEA inspectors to monitor the freeze. IAEA inspectors returned to Yongbyon and related facilities, including the partially built 50 and 200MW nuclear power plants. Immediately following the return of IAEA monitoring teams, friction developed between inspectors and North Korean authorities. Over a span of six years, nearly 20 technical conferences failed to produce North Korean cooperation in resolving key monitoring issues.

**The 2002–2003 crisis.** In 1999, IAEA officials reported to the United Nations Security Council that “critical parts” of the North Korean reactor at Yongbyon had been unaccounted for since 1994. Missing parts included those needed to control nuclear reactions and/or those that would be needed to construct another nuclear reactor.

In 2000, the United Nations Secretariat determined that it would take at least three years to complete verifications that had been pending for nearly a decade. North Korea ignored the United Nations and failed to even discuss a timeframe for resolving outstanding issues at technical meetings in November 2001. The following year, while the United States was preoccupied diplomatically and militarily with a developing crisis in Iraq, North Korean

leaders demanded that the United States once again enter into unilateral negotiations regarding nuclear arms proliferations issues. The demand for talks was widely interpreted by news agencies and diplomatic corps personnel in the United States as a signal that North Korea—facing desperate economic conditions and starvation for a significant portion of its population—sought additional concessions, money, and aid from the United States. President George W. Bush’s administration declined the offer for unilateral talks and vowed not to succumb to “nuclear blackmail” by North Korea. In October 2002, North Korean officials announced that, in violation of the Framework Agreement with the United States, their government had a secret program to “enrich uranium for nuclear weapons.”

Ongoing negotiations between North Korea and South Korea in Pyongyang stalled because of North Korea’s nuclear program admissions. United States Secretary of State Colin Powell warned that further aid to North Korea under the 1994 Framework Agreement was in danger. In exchange for North Korea allowing inspections and discontinuing efforts to develop nuclear weapons, the United States (through the KEDO Board) had agreed to supply fuel for conventional electrical generation and to facilitate the construction of two safe lightwater nuclear power reactors (LPRs). Construction of the first LPR had been started in 2000 and was scheduled for completion in 2005. Diplomatic efforts stalled, and in response the United States and KEDO Board announced that they would suspend heavy oil shipments to North Korea.

In December 2002, North Korea informed IAEA inspectors that the freeze on nuclear facility use would be lifted. North Korea also announced their intent to remove IAEA seals and disable surveillance cameras. Removal of those seals and the dismantling of IAEA monitoring equipment began in late December 2002 and on December 27, North Korea ordered IAEA inspectors to leave the country. On January 11, 2003, North Korea announced its withdrawal from the Nuclear Non-Proliferation Treaty. The United States and United Nations continued to insist that North Korea’s prior NPT agreement remained binding and enforceable.

Scientists and intelligence experts openly doubted North Korea’s claims that its nuclear program was designed solely to produce electricity. Experts cited the fact that the Yongbyon reactor was too small for significant power generation. Experts also argued that by restarting its nuclear program, North Korea could produce enough plutonium for five or six nuclear bombs within a few months. The IAEA issued the following statement: “Restarting this now unsafeguarded nuclear facility will further demonstrate the DPRK’s disregard for its nuclear non-proliferation obligations.”

**Intelligence and political estimates of North Korean capabilities and motives.** The C.I.A. has warned that North Korea

may already have two nuclear weapons—possibly developed before the 1994 nuclear freeze accord. What United States officials more openly fear is that nuclear fuel might be sold by North Korea to terrorist organizations that seek to build nuclear weapons to use against the United States.

In addition, North Korea has started a series of missile tests with the goal of demonstrating that North Korea could build a rocket capable of reaching the western coast of the United States. In 2002 North Korea heightened tensions in the region with a launch of a ballistic missile over Japanese territory.

In February 2003, North Korea announced that its nuclear facilities were fully reactivated. The North Korean program included known sites at Yongbyon (a 5 MW experimental nuclear power reactor and a partially completed plutonium extraction facility), Taechon, Pyongyang, and the LPRs being built at Kumho. The IAEA announced that North Korea was in breach of its agreements and referred the matter to the United Nations Security Council.

The rhetoric and tensions continued to escalate. North Korean dictator Kim Jong-Il warned that any U.S. strike against its nuclear facilities at Yongbyon would trigger “full-scale war.” North Korea maintained a standing army of more than one million soldiers. America maintained less than 40,000 troops in South Korea. Some western intelligence sources openly speculated that North Korea possessed one or two operational nuclear weapons, as well as enough spent fuel rods to make additional weapons.

Despite North Korean threats of pre-emptive action and heavy troop commitments to the Middle East in anticipation of having to forcefully disarm a defiant Iraq, the United States sent reinforcements in the form of heavy bombers and naval vessels toward the Korean peninsula.

In early March 2003, four North Korean fighter jets intercepted a United States reconnaissance plane in international air space. The jets followed the reconnaissance plane and locked on with targeting RADAR. (In 1969, a United States reconnaissance plane was shot down under similar circumstances.) Ultimately the U.S. plane returned safely to base.

After ignoring yet another missile firing by North Korea, United States officials insisted that they intended to pursue a policy that would put “maximum pressure” on North Korea to “not just freeze its weapons of mass destruction, but begin to dismantle them.” Bush administration officials—in referring to the failed unilateral agreement reached between the U.S. and North Korea in 1994—consistently asserted that North Korea froze its plutonium program, it then began a separate uranium enrichment program. The United States maintained that a solution to the crisis needed to come from pressure and influence applied by the “collective weight of the international community, not just from the United States alone.” Secretary of State Colin Powell articulated the American position by stating “We can’t fall into that trap again of paying them off to stop what they’re doing, only to discover that they’re doing it again at a later time.”

Tensions also escalated between allies as anti-American demonstrations began taking place in South Korea. Fueled in part by a general global anti-American backlash over the anticipated war against Iraq the demonstrations were mainly fears that America’s failure to renounce the option of a military strike against North Korea might escalate into a devastating war in the Korean peninsula. After having secured South Korea’s independence at the cost of many American lives and following more than 50 years of commitment to the country’s security, the South Korean protests were an affront to the United States and forced administration and defense officials to publicly ponder the possibility of reducing or removing American forces.

The Bush administration continued to downplay the crisis and insisted that it was a regional matter to be solved by joint diplomacy rather than unilateral talks. In late April 2003, the first round of talks on the crisis began as American, North Korean, and Chinese officials met in Beijing.

As of May, 2003, IAEA inspectors asserted that they had never been able to verify the completeness and correctness of even the initial report of North Korea with regard to its NPT Safeguards Agreement. Since 1993, the IAEA has maintained that North Korea was in “non-compliance” with its obligations under NPT and inspection agreements to verify the peaceful use of its nuclear materials.

#### ■ FURTHER READING :

##### BOOKS:

- Michael Mazarr, M. *North Korea and The Bomb: A Case Study in Nonproliferation*. New York: St. Martin’s Press, 1995.
- Oberdorfer, Don. *The Two Koreas: A Contemporary History*. Reading, MA: Addison-Wesley, 1997.
- Sigal, Leon V. *Disarming Strangers: Nuclear Diplomacy with North Korea*. Princeton, NJ: Princeton University Press, 1998.

##### PERIODICALS:

- Gordon, M. R. “U.S. Nuclear Plan Sees New Targets and New Weapons.” *New York Times*, March 10, 2002.
- Loeb, Vernon, and Peter Slevin. “Overcoming North Korea’s ‘Tyranny of Proximity.’” *Washington Post*. January 20, 2003.
- Sanger, David E. “U.S. Eases Threat On Nuclear Arms For North Korea.” *New York Times*. December 30, 2002.

##### ELECTRONIC:

“Beyond the Agreed Framework: The DPRK’s Projected Atomic Bomb Making Capabilities, 2002–09.” An Analysis of The Nonproliferation Policy Education Center (NPEC) (December 3, 2002) <<http://www.npec-web.org/projects/fissile2.htm>>. December 12, 2002.

IAEA News Update on IAEA and North Korea. IAEA (March 10, 2003) <<http://www.iaea.org/worldatom/Press/Focus/laeaDprk/>> (March 10, 2003).

"North Korea Nuclear Profile." Center for Nonproliferation Studies. <[http://www.nti.org/db/profiles/dprk/nuc/nuc\\_overview.html](http://www.nti.org/db/profiles/dprk/nuc/nuc_overview.html)> (January 12, 2003).

Pinkston, D., and S. Lieggi. "North Korea's Nuclear Program: Key Concerns." Center for Nonproliferation Studies, <<http://cns.miis.edu/research/korea/keycon.htm>> (December 12, 2002).

#### SEE ALSO

*Air Plume and Chemical Analysis  
North Korea, Intelligence and Security  
Nuclear Detection Devices  
Nuclear Reactors  
Nuclear Weapons*

---

## Norway, Intelligence and Security

---

During World War I, Norway maintained a stated policy of neutrality in international affairs. When WWII erupted in 1939, the Norwegian government again asserted that the nation would remain neutral in the conflict. However, on April 9, 1940, the German army invaded Norway. The Gestapo and Abwehr established intelligence bases in Norway to monitor radio and wire traffic from Britain, the Soviet Union, and the North Atlantic. Members of the Norwegian government who were able to escape fled to Britain. This group of refugees included members of the Norwegian intelligence services. Many of them aided British Military Intelligence with data collection, cartography, and cryptography operations.

Today, Norway's intelligence service is dominated by the Control Committee for the Intelligence and Security Services. The Control Committee coordinates intelligence operations, collects and analyzes intelligence information, assesses national security threats, and briefs government officials on intelligence matters. Staffed predominantly by civilian government intelligence personnel, the Control Committee also employs military officers to foster cooperation between Norway's main intelligence agencies and smaller, specialized military intelligence units.

The Joint Defense Intelligence Service (FE) is responsible for most Norwegian intelligence operations, including signals, communications, electronic, and human intelligence. Although the stated mission of the FE includes assessing and thwarting both external and internal threats to national security, the FE concentrates mainly on foreign intelligence.

Domestic intelligence, as well as the coordination with law enforcement agencies of protective services for Norwegian diplomats and national interests, is the chief task of the Joint Defense Security Service (FS). The FS often works closely with the Police Intelligence Service

(PO) to investigate high crimes, such as money laundering, illegal trafficking, and business corruption. The two agencies also maintain counter-intelligence units.

Norway has since eased its hard-line stance on neutrality. While Norway abstains from membership in the European Union, it did join the North Atlantic Treaty Organization (NATO). Though Norway has participated in several NATO intelligence and military operations, the Norwegian government insists that military bases in the country cannot be used by foreign powers unless Norway is under threat of attack. Norway also maintains restrictions on its territorial waters, even for NATO allies. Norway is also a member of the Organization for Security and Cooperation in Europe (OSCE) and the Council of Baltic Sea States.

Norway pledged intelligence and limited military support for the recent international campaign against terrorism. In 2002, The Norwegian government authorized the deployment of military Special Forces for participation in the United States-led Operation Enduring Freedom in Afghanistan.

#### SEE ALSO

*European Union*

---

## NRO (National Reconnaissance Office)

---

The National Reconnaissance Office (NRO) is a member of the United States' fourteen-member intelligence community. Established in 1960, the existence of the NRO was not declassified until 1992. The NRO collects and analyzes satellite and airplane reconnaissance information for various military and civilian intelligence agencies. As part of this mission, the NRO also researches, designs, and deploys reconnaissance satellites.

Although the NRO is a Department of Defense agency, the Director of Central Intelligence and the Secretary of Defense share control over the agency. Members of the Central Intelligence Agency (CIA) and the Department of Defense staff the NRO. The Under Secretary of the Air Force serves as the Director of the NRO and reports directly to the Secretary of Defense. However, the Secretary of Defense must nominate the Under Secretary of the Air Force in conjunction with the Director of Central Intelligence. The Senate must confirm the nomination. Six Congressional Committees oversee NRO operations.

Although the United States was already developing a space-based reconnaissance program, the Eisenhower administration shook up the organization of this program following the downing of Gary Powers' U-2 spy plane by



the Soviet Union in May, 1960. Because of the Powers' incident, the Eisenhower administration quickly formed a committee to examine the continuation of America's high-altitude and space-based intelligence gathering capabilities.

In August, 1960, Secretary of Defense Thomas Gates presented his committee's findings to the National Security Council. Secretary Gates recommended the formation of an agency that would balance the intelligence concerns of both civilian intelligence agencies and the military. Based on the Gates committee findings, the Eisenhower and Kennedy administrations worked with the Department of Defense, the CIA, and the Air Force to develop the NRO.

By 1961, control of the NRO fell to the CIA and the Department of Defense, represented by the Air Force. This power-sharing arrangement has been the source of conflicts, as each agency has advocated its specific agenda. In the early 1960s, budgetary concerns and competing interests led to clashes between the CIA and Air Force for control of the NRO. The Air Force wanted the NRO to assist in military operations and tactics, while the CIA believed that the primary role of the NRO should be to protect national interests.

These conflicts led to the development of several splintered programs in the NRO. Major reorganizations of the NRO in 1989 and 1992 centralized command of the program under the Director of the NRO. Many critics, however, argue that the effectiveness of the NRO still suffers because of these competing interests. With a substantial budget at stake each year, technological advancements tend to focus too heavily on the development of new satellite systems, some critics claim, while advancements in data analysis often suffer.

During the Cold War, the NRO's primary concern was tracking the troop, plane, and missile deployments of the Soviet Union and its satellite states. After its formation, the NRO took over administration of CORONA, the world's first photo reconnaissance satellite. The CORONA program, declassified in 1995, operated from August, 1960 until May 1972. During its twelve years, CORONA took over 800,000 images.

After the Cold War, the NRO shifted its mission to better assist in intelligence gathering in regional conflicts. The NRO provided crucial information to military and civilian intelligence agencies during the coalition efforts in the Gulf War in 1991 and United States and NATO operations in the Balkans. Following the collapse of the Soviet Union, the NRO also focused much of its energy on tracking the smuggling of nuclear weapon components.

Since September, 2001, the NRO has played an increased role in the effort to combat terrorism. NRO satellite information assists the intelligence community in identifying suspected terrorist training camps, tracing arms shipments, and searching for the development of weapons of mass destruction by terrorists and rogue nations. By providing military and civilian intelligence agencies with information on developments in these areas, the

NRO's mission is to use satellite reconnaissance to prevent attacks against the United States military, economy, infrastructure, and civilians.

#### ■ FURTHER READING:

##### ELECTRONIC:

United States National Reconnaissance Office. <<http://www.nro.gov>> (May 2003).

##### SEE ALSO

*Satellites, Spy*

---

## NSA (United States National Security Agency)

---

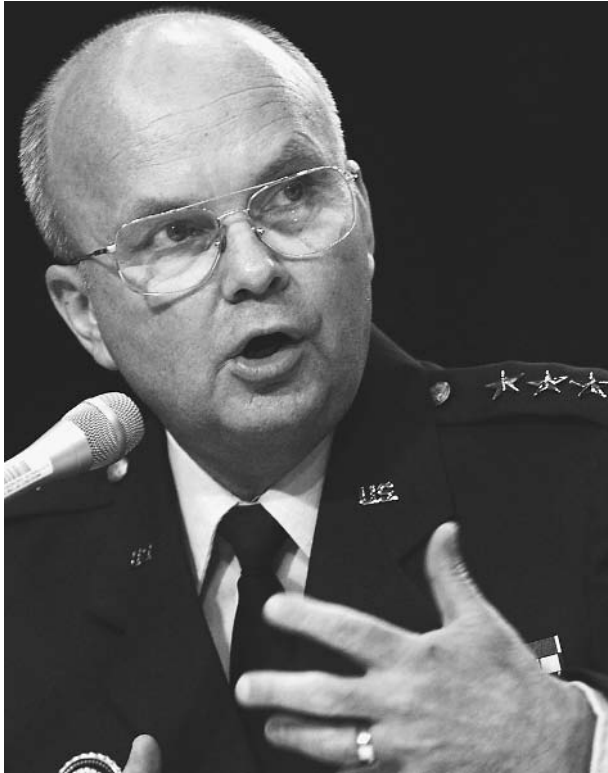
#### ■ JUDSON KNIGHT

Legendary for its secrecy, the National Security Agency (NSA) is the leading cryptologic organization in the United States intelligence community. Focused on cryptologic and cryptanalytic missions, it is the nation's leading employer of mathematicians, yet little is known about the inner workings of this secretive agency. Those few details in the public domain have come either through treachery (namely, revelations made public by defectors in the early 1960s) or the tireless efforts of a writer, James Bamford, whose 1982 book *The Puzzle Palace: A Report on America's Most Secret Agency* was the first detailed study of the NSA.

### NSA and the Cold War

NSA's creation in 1952 followed years of efforts to coordinate communications intelligence (COMINT) activities by U.S. forces. The creation of the Armed Forces Security Agency (AFSA) in 1949 seemed to solve this problem, but the experience of cryptologic services early in the Korean War revealed that it had not. Instead of replacing the cryptologic operations of the U.S. Army, Navy, and Air Force, AFSA clashed with these, and rather than take the lead, it simply became a fourth military cryptologic operation.

The result was a secret memorandum by President Harry S. Truman, National Security Council Intelligence Directive (NSCID) No. 9, issued on October 24, 1952. Although the bulk of NSCID 9 has never been made public, it is clear that this document established NSA to take the lead position in COMINT operations. The choice of "national" in the organization's title emphasized the fact that it would serve both military and nonmilitary needs, and instead of reporting to the Joint Chiefs of Staff, the head of



National Security Agency Director Lt. General Michael Hayden answers questions about what went wrong prior to the September 11, 2001, attacks before the Senate Select Committee on Intelligence, October 17, 2002. ©REUTERS NEWMEDIA INC./CORBIS.

NSA would answer to the Secretary of Defense. The Secretary, in turn, delegated all his COMINT responsibilities to the Director, NSA, as that position was thenceforth known. AFSA, though not officially abolished by NSCID 9, simply faded away.

**Revelations.** For years, Americans had almost no idea as to the workings of the NSA. Then, in September 1960, NSA cryptographers William H. Martin and Bernon F. Mitchell held a news conference in Moscow to announce their defection. They proceeded to divulge a number of previously secret details about NSA, including the fact that it monitored communications from and in more than 40 countries, including not only members of the Warsaw Pact, but also putative U.S. allies such as France. Three years later, a third NSA defector, research analyst Victor N. Hamilton, told the Soviet newspaper *Izvestia* that NSA was in the process of breaking numerous countries' diplomatic codes and ciphers. He also revealed that NSA had been intercepting communications to and from specific nations' missions at United Nations headquarters in New York City.

In light of these experiences, occurring as they did against the backdrop of the Cold War at its height, it is perhaps not surprising that NSA reacted with hostility to

legitimate scholars writing on ciphers and codes or the organization itself. The first of these was David Kahn, an amateur cryptologist whose 1967 book *The Codebreakers* came so close to revealing NSA cryptologic methodology that the agency tried to stop its publication. When it did finally appear, it was published by a British publishing house. Fifteen years later, Bamford used the access granted by the Freedom of Information Act to write *The Puzzle Palace*. A book whose publication NSA opposed with even greater vigor than it had *The Codebreakers*, Bamford's work was the first full-scale study of NSA, and one of the few that exists even today.

**NSA today.** Though today's NSA is far from an open book, several of its actions in the 1990s reveal a much greater degree of openness in the post-Cold War environment. During the mid-1990s, the agency opened both a Center for Cryptologic History and a National Cryptologic Museum, the latter located near its Fort Meade, Maryland, headquarters in a former motel that NSA purchased years before to prevent enemies from using it as a listening post. Kahn and Bamford, once anathema to the agency, had gained new respect: Kahn was given a position as visiting distinguished historian at the Center for Cryptologic History, while Bamford received full cooperation from NSA when writing a second book about the agency.

The title of that book—*Body of Secrets: Anatomy of the Ultra-Secret National Security Agency: from the Cold War Through the Dawn of a New Century* (2001)—might seem a bit incongruous in light of NSA's new openness, but in this case, "openness" is a relative term. NSA remains highly secretive about its operations, and even the most minor of its civilian employees is subject to extensive scrutiny and oversight. Plans to marry a foreign citizen—even if the person marrying is not the employee *but a relative of the employee*—must be announced to supervisors. The same is true of plans for travel overseas, and those who fail to comply are presumably fired, though not before extensive checks determine whether they passed secrets to an enemy. Even the physicians an employee visits must be on an approved list, in case the employee reveals sensitive secrets under anaesthesia.

Some 20,000 people work at the NSA's 650-acre campus at Fort Meade, making this organization the largest employer in Maryland. The Fort Meade facility includes the National Cryptologic School, a vast printing plant, and a massive factory producing computer chips. The chips are used at the heart of NSA operations, the supercomputers at Fort Meade, where codes and ciphers are made and broken. In the mid-1990s, NSA was estimated to have an annual budget of \$3.5 billion.

In addition to the 20,000 at Fort Meade, up to an estimated 100,000 other personnel, mostly military, work for NSA in other parts of the world. The director of NSA is a three-star general or admiral experienced at intelligence work. He also serves as head of an agency within the agency, the Central Security Service (CSS), which is even

more secretive than NSA itself. Tasked with providing information security to U.S. communications and cracking the codes of other nations, CSS was established in 1972. Nesting within it, at a still deeper layer of secrecy, is the Special Collections Service, an elite unit devoted to listening in on communications in countries hostile to the United States.

Under the control of NSA is a vast global network of ground stations, ships, aircraft, and satellites that together give it an almost supernatural aura of omniscience. This aura is more than a matter of mere reputation or hype: NSA itself estimates that several times a day, it processes more information than is contained in all the volumes in the Library of Congress. Among the most impressive of its surveillance programs is Echelon, through which NSA, working with other intelligence services in the English-speaking world, monitors communications throughout Europe.

#### ■ FURTHER READING:

##### BOOKS:

Bamford, James. *The Puzzle Palace: A Report on America's Most Secret Agency*. Boston: Houghton Mifflin, 1982.

———. *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency: From the Cold War through the Dawn of a New Century*. New York: Doubleday, 2001.

Kahn, David. *The Codebreakers*. London: Weidenfeld and Nicholson, 1967.

Richelson, Jeffrey T. *The U.S. Intelligence Community*, 4th ed. Boulder, CO: Westview Press, 1999.

##### ELECTRONIC:

National Security Agency. <<http://www.nsa.gov/>> (March 24, 2003).

National Security Agency. Federation of American Scientists. <<http://www.fas.org/irp/nsa/index.html>> (March 24, 2003).

##### SEE ALSO

*COMINT (Communications Intelligence)*  
*Satellites, Spy*  
*SIGINT (Signals Intelligence)*  
*Special Collection Service, United States*

---

## NSC (National Security Council)

---

#### ■ JUDSON KNIGHT

Established by the National Security Act of 1947, the National Security Council (NSC) was intended to serve as the principal advisory board for the president of the United

States on matters of national security and foreign policy. In practice, the importance of the NSC and the National Security Advisor has depended on the degree of power the chief executive accords to it. The NSC consists of four statutory members—president, vice president, and secretaries of State and Defense—along with two statutory advisors, the Chairman of the Joint Chiefs of Staff and the Director of Central Intelligence. Other officials participate as requested.

### Presidents and their NSCs

The 1947 National Security Act became Public Law 235–61 Stat. 496; U.S.C. 402. Two years later, Congress passed the National Security Act Amendments of 1949 (63 Stat. 579; 50 U.S.C. 401 et seq.) These amendments led to a reorganization plan whereby the NSC became part of the executive office of the president. Whereas Congress and the departments of State and Defense had each sought to place the new council under their control, thenceforth—assuming it had any role at all—the NSC would be under the leadership of the president.

Harry S. Truman, the first president with an NSC, made little use of the council, but Dwight D. Eisenhower relied heavily on the NSC. John F. Kennedy, on the other hand, placed little emphasis on the NSC as such, but relied heavily on the first of many powerful National Security Advisors, McGeorge Bundy. In subsequent administrations, the emphasis on the NSC itself has shifted, but the president's reliance on the National Security Advisor seems to be a constant.

Democratic presidents, including Lyndon B. Johnson, James E. Carter, and William J. Clinton, have tended to approach the NSC with distrust upon entering office, and to supplant its functions with outside committees thereafter. Nevertheless, each relied heavily on National Security Advisors, including Bundy in Johnson's early years, Zbigniew Brzezinski throughout Carter's term, and Samuel "Sandy" Berger in Clinton's second term.

**Republican administrations.** Republicans, by contrast, have typically entered office with a positive view of the NSC itself, or at least of the National Security Advisor's role. In the administration of Richard M. Nixon, the NSC itself played little role, but NSC Advisor Henry Kissinger was perhaps second only to Nixon in power during the early 1970s. As Nixon's influence waned due to the Watergate scandal, Kissinger's importance continued into the administration of Gerald R. Ford.

The NSC of Ronald Reagan took an extremely activist role in overseas affairs, to such an extent that this led to another scandal, the Iran-Contra affair. National Security Advisor Robert McFarlane and his successor, Admiral John Poindexter, played key roles in fomenting the scheme to sell arms to the Iranian fundamentalist regime in exchange for the release of hostages, and to direct proceeds from these sales to the anticommunist Contras in Nicaragua.



President Bush sits with his National Security Council during a meeting in the Cabinet Room of the White House, September 12, 2001. From left to right, Secretary of State Colin Powell, President Bush, Vice-President Dick Cheney, and Chairman of the Joint Chiefs of Staff General Henry Shelton. AP/WIDE WORLD PHOTOS.

After Poindexter's departure, Reagan appointed Lieutenant General Colin Powell, who ran a tight, no-nonsense NSC. George H. W. Bush, who made Powell Chairman of the Joint Chiefs of Staff, appointed Brent Scowcroft as National Security Advisor. Scowcroft, who had directed the NSC after Kissinger left the position in 1975, was known for his warm relations with other centers of power around the president—including the National Security Advisor's two traditional rivals for the president's ear, the secretaries of Defense and State. This collegial tradition continued in the administration of George W. Bush, as National Security Advisor Condoleezza Rice worked closely with Secretary of State Powell and Secretary of Defense Donald Rumsfeld in the war on terror.

**NSC members.** The chairman of the National Security Council is the president, who relies to varying degrees on the National Security Advisor. The position of the latter, whose

official title is Assistant to the President for National Security Affairs, is not mentioned in the original legislation, and in fact the role of National Security Advisor emerged only during the Kennedy administration.

In addition to the four statutory members, the two statutory advisors on military and intelligence affairs, and the National Security Advisor, the Secretary of the Treasury is a regular attendee at NSC meetings. The Chief of Staff to the President, Counsel to the President, and Assistant to the President for Economic Policy are invited to attend any NSC meeting, while the Attorney General and the Director of the Office of Management and Budget are invited to attend those meetings that pertain to their responsibilities.

The directors of other executive departments and agencies, as well as other senior officials, are invited to attend meetings of the NSC when appropriate. Among those holding positions created by latter-day presidents:

the National Economic Advisor, established by Clinton, and the Secretary of Homeland Security, a Cabinet-level post created by George W. Bush in the wake of the September 2001 terrorist attacks. The first of these directs the National Economic Council, which works closely with the NSC and with presidential advisors who report to the National Security Advisor.

#### ■ FURTHER READING:

##### BOOKS:

- Best, Richard A. *The National Security Council: An Organizational Assessment*. Huntington, NY: Novinka Books, 2001.
- Crabb, Cecil Van Meter, and Kevin V. Mulcahy. *American National Security: A Presidential Perspective*. Pacific Grove, CA: Brooks/Cole, 1991.
- Hillen, John. *Future Visions for U.S. Defense Policy: Four Alternatives Presented as Presidential Speeches*. New York: Council on Foreign Relations, 1998.
- Leitzel, Jim. *Economics and National Security*. Boulder, CO: Westview Press, 1993.
- Lord, Carnes. *The Presidency and the Management of National Security*. New York: Free Press, 1988.

##### ELECTRONIC:

National Security Council. <<http://www.whitehouse.gov/nsc/>> (March 24, 2003).

##### SEE ALSO

*National Security Act (1947)*  
*National Security Advisor, United States NSC (National Security Council), History*  
*President of the United States (Executive Command and Control of Intelligence Agencies)*

---

## NSC (National Security Council), History

---

#### ■ JUDSON KNIGHT

The history of the United States National Security Council (NSC) lends itself to widely diverging views of the NSC, depending on the presidential administration in question. Held in suspicion by President Harry S. Truman, the organization became a vital part of the Dwight D. Eisenhower administration. Thereafter it remained, for the most part, a significant aspect of subsequent administrations, although in differing manners. For example, four very different chief executives—John F. Kennedy, Richard M. Nixon, James E. Carter, and George W. Bush—relied heavily on powerful National Security Advisors (McGeorge Bundy,

Henry Kissinger, Zbigniew Brzezinski, and Condoleezza Rice, respectively), yet the similarities in organizational style end there.

### The Roots of the NSC (1947–53)

Among its many provisions, which collectively reformed the U.S. defense, intelligence, and security apparatus, the National Security Act of July 26, 1947, created the NSC. The latter was to serve as a presidential advisory board on issues of significance to the military, security, intelligence, and foreign policy. Its chairman would be the president, and its members would include the secretaries of State, Defense, the Army, Navy, and Air Force, as well as the director of the National Security Resources Board. Other Cabinet-level secretaries and officials with prominent security roles could attend occasionally. The Central Intelligence Agency (CIA), also created by the National Security Act, was to report to the NSC in an advisory role, but the Director of Central Intelligence (DCI) was not an NSC member.

The enabling legislation, designated as Public Law 80–253, made no mention of the National Security Advisor, a figure whose role would become prominent only in the Kennedy years. However, there was a powerful precedent for the idea of trusted White House advisors as guides for national policy; during World War II, President Franklin D. Roosevelt had depended on top White House aides such as Harry Hopkins and Admiral William D. Leahy at least as much as he did on his Cabinet secretaries. Likewise, during the early years of his administration, President Truman enjoyed a similar rapport with Special White House Counsel Clark Clifford.

This relationship with Clifford coexisted with Truman's ambivalence toward the NSC. Wary of a surfeit of advice and advisors that could impair his ability to make executive decisions, Truman largely ignored the NSC until the outbreak of the Korean War, attending only 10 of 55 meetings in those first three years of the body's existence. In 1949, however, Truman signaled a new interest in it when he instructed the Secretary of the Treasury to attend all NSC meetings. Congress also amended the earlier act to remove the three service secretaries, who would be represented thenceforth by the Secretary of Defense. The amendment also added the vice president to the Council, and made the Joint Chiefs of Staff (JCS) permanent advisors on military matters.

Other events of 1949—the formation of the North Atlantic Treaty Organization, Soviet detonation of an atomic bomb, the Communist takeover in China—all signaled a growth in importance for the Council, but the real change came after the outbreak of hostilities in Korea in June 1950. Thereafter, Truman, although he continued to rely on other sources for advice, attended most NSC meetings. Through the Council, he authorized the first of what were to be many covert operations on the part of the U.S. intelligence community.



President Lyndon Johnson (right side, second from right) shown meeting with the National Security Council in 1964 with the prime topic expected to be the North Vietnamese torpedo boat attack on the U.S. destroyer Maddox. ©BETTMANN/CORBIS.

## The Eisenhower Years (1953–61)

As a former general, Eisenhower came to the White House with an appreciation for advisory staffs and for the organized system of strategic planning that the NSC concept embodied; therefore, the Council flourished under his administration. So, too, did various study groups, headed by the Operations Coordinating Board (OCB), which included the Undersecretary of State for Political Affairs, the Deputy Secretary of Defense, DCI, and others. Eventually, there would be more than 40 interagency working groups, and critics of the Eisenhower NSC complained that it was bogged down by too many committees and excess reports.

At the heart of the NSC were four full-time statutory members: the president, vice president, and the secretaries of State and Defense. Along with the Director of the Office of Defense Mobilization, these formed the core of the Eisenhower NSC. The Treasury Secretary, JCS Chairman, DCI, and others regularly attended meetings. Eisenhower created the position of Special Assistant for National Security Affairs, forerunner of the modern National Security Advisor, but in the 1950s this job was chiefly that of a staff coordinator, with little independent power.

A hands-on leader, Eisenhower attended the vast majority of NSC meetings—329 out of 366—that took

place during his eight years in office. NSC meetings were the single most significant regularly recurring item on his weekly agenda, and through the Council he closely oversaw a burgeoning roster of covert missions, most notably in Iran in 1953 and Guatemala in 1954. His emphasis on the NSC had many detractors, among them Secretary of State John Foster Dulles, who naturally feared that the Council would eclipse his own importance in foreign policy; Senator Henry Jackson, chairman of the Senate Subcommittee on National Policy Machinery (1960–61); and others.

## Kennedy and Johnson (1961–69)

The report of Jackson's subcommittee had a strong effect on Kennedy, who, upon assuming leadership in 1961, immediately cut NSC staff from 74 to 49. He also reduced the number of substantive members, and the frequency of their meetings. Therefore, it is ironic that Kennedy would ultimately strengthen the NSC by establishing the position of National Security Advisor, and by appointing Bundy—already a closely trusted associate—to the job.

The apparent contradiction in Kennedy's position on the NSC is explained by the aftermath of the disastrous Bay of Pigs invasion, an abortive April 1961 attempt to wrest control of Cuba from Communist dictator Fidel

Castro. In Kennedy's view, the State Department failed to effectively orchestrate the White House response to the debacle, so he turned to Bundy and the NSC for this assistance.

In 1962, NSC gained a powerful tool, both symbolic and real, for its implementation of policy when the Situation Room was established in the White House basement. The Sit Room, as it was called, connected the President with State, Defense, and the CIA, while providing the National Security Advisor with an opportunity to monitor cables from foreign service posts around the world.

Kennedy remained ambivalent toward the NSC as such, which met only 49 times in his three years as president. Much of its work was replaced by the Standing Group, which consisted of Bundy, DCI, the Deputy Secretary of Defense, and the Undersecretary for Political Affairs, who served as its chair.

As crises developed during the course of Kennedy's tenure in the White House, the President or Bundy established committees to respond to them. This was in sharp contrast to Eisenhower's emphasis on long-range planning, but sometimes these ad hoc groups outlasted their original purposes, and continued to serve in planning for the future.

For example, the Executive Committee of the National Security Council, formed as the Cuban Missile Crisis was heating up in the early fall of 1962, continued to meet until the spring of the following year. During that time, its agenda included a number of items besides Cuba. Kennedy also formed the 5412 Committee to oversee covert operations. Although chaired by Bundy, the committee operated outside the NSC framework.

This reliance on ad hoc committees was one of several practices that would continue under Lyndon B. Johnson when he assumed leadership after Kennedy's assassination in November, 1963. In February, 1965, as the war in Vietnam was reaching its height, Johnson convened the NSC frequently, but after that month, it seldom met. When it did, its role was to simply approve actions decided by the White House rather than to direct policy.

Also like Kennedy, Johnson's antipathy toward the NSC contrasted with his reliance on the National Security Advisor. Bundy remained in that position until February 1966, when he was replaced by Walt Rostow. The National Security Advisor, along with Secretary of State Dean Rusk and a few other key figures, met with the President for lunch almost every Tuesday from February 1964 onward, and this "Tuesday Lunch Group" largely performed the advisory role for which the NSC had been designed.

## Nixon, Ford, and the Kissinger Era (1969–77)

Two names from the Nixon era epitomize the emphasis he placed on the role of the National Security Advisor: Henry

Kissinger and William Rogers. Kissinger was Nixon's National Security Advisor, while Rogers served as Nixon's first Secretary of State. Nixon went into office intending to direct foreign policy from the White House with the aid of a highly effective National Security Advisor. Therefore, to avoid conflicts with the State Department, he appointed a virtual unknown and inexperienced diplomat to its top position.

Kissinger would replace Rogers as Secretary of State in September 1973, becoming the only person in history to hold that position while remaining National Security Advisor. By then, the power of Kissinger himself, magnified by the eclipse of Nixon in the Watergate scandal, was far greater than the influence formally accorded to any government position. Under Gerald R. Ford, who succeeded Nixon after his resignation in August 1974, Kissinger relinquished his dual role when Lieutenant General Brent Scowcroft became National Security Advisor in November 1975. Kissinger remained the President's chief advisor, however, and Scowcroft deferred to Kissinger as the leading figure in foreign policy.

Kissinger relied on a number of planning and review committees to help him manage an ever-widening array of issues that included Vietnam, rising tensions in the Middle East, efforts toward normalization of relations with China, and the birth of detente with the Soviet Union. This necessitated expansion of the NSC staff from 12 to 34 members, as well as other measures. Through his secretary, Jeanne Davis, he instituted a computerized document-tracking system, a revolutionary move in the 1970s. With the help of the White House Communication Agency, which had special aircraft that operated as communication centers, Kissinger could travel the globe, operating a one-man command post.

So great was his power that his accession to the top position at the State Department in 1973 was more of an annoyance to Kissinger than anything else; as he later recalled in his memoirs, serving in dual roles forced him into the inherently ridiculous position of having to represent the Department of State's interests at the NSC. For this reason alone, aside from more obvious concerns about one person having too much power, it is unlikely that both positions will again be held by the same person at the same time.

## The Carter Interregnum (1977–81)

James E. Carter acceded to the presidency in January 1977 with a promise to reform many of the excesses that had darkened Washington. Among these was the virtually unprecedented accumulation of power by Kissinger, which he sought to counteract by returning the NSC to a role of policy coordination and research. Once again, the NSC staff was cut, this time reduced by half. For his National Security Advisor, however, Carter chose another strong personality, Zbigniew Brzezinski.

Carter also allowed the growth of new committees, which replaced those of the Kissinger era. Brzezinski chaired only one of the two principal NSC committees, the Standing Coordinating Committee, and thus Carter hoped to hold the NSC's influence in check. These committee meetings ultimately formed the basis for presidential directives, classified orders from the White House that originated with Nixon.

The NSC as a whole met only 10 times in Carter's four years, a far cry from the 125 meetings of the eight years of Republican administrations that preceded his. Like his Democratic predecessors, Carter relied instead primarily on informal and ad hoc groups. Whereas Johnson had his Tuesday lunches, Carter had his Friday breakfasts, at which he met with Vice President Walter Mondale, Secretary of State Cyrus Vance, Secretary of Defense Harold Brown, Brzezinski, and others.

Despite Carter's efforts to prevent the rise of another Kissinger, Brzezinski soon emerged as a leading figure of his administration. Differences between Brzezinski and Vance, combined with the lack of strong leadership from the top, helped spawn the series of foreign-policy debacles that would help bring the Carter years to an end. Whereas Brzezinski favored taking a strong, activist stance toward U.S. enemies—the Soviets who had invaded Afghanistan, and the fundamentalists who had seized control of Iran—Vance took a more cautious position. These differences in approach came to a head during the abortive March 1980 attempt to rescue the U.S. hostages from Iran. Conceived by Brzezinski, the move was submitted to so many changes in an effort to ameliorate all sides (a fact symbolized by the multiservice team undertaking the attempted rescue) that it ultimately lacked the clear direction essential to such a bold move. In the wake of the hostage-rescue disaster, Vance resigned, and Carter's fate in the coming election was sealed.

## Ronald Reagan and George H. W. Bush (1981–93)

Seeing Carter's failure to resolve the rivalry between NSC and the State Department, as a presidential candidate, Ronald Reagan called for a decrease in the power of the National Security Advisor. On the day of Reagan's inauguration, his Secretary of State, Alexander Haig, drafted a presidential directive placing all foreign-policy planning under his own department. It seemed that the problem had been resolved, but in fact a new one had been created, because other members of the Reagan administration feared that the new direction of foreign policy took too much power away from the president.

Reagan, however, was determined to reduce the power of the NSC, and he directed National Security Advisor Richard Allen to report to presidential advisor Edwin Meese. This marked the first time since the inception of the NSC that the National Security Advisor did not have a direct

line of contact with the President. Meese chaired a meeting in February 1981, that revived senior interdepartmental groups (SIGs), first introduced under Johnson. The meeting established three SIGs, on foreign, defense, and intelligence issues, that would be chaired by the secretaries of State and Defense and the DCI, respectively.

Allen resigned in January 1982, and Reagan replaced him with Deputy Secretary of State William Clark, a close friend. Thenceforth the National Security Advisor would again hold a powerful role. There followed a series of presidential directives and other orders clarifying the functions of the advisor and the SIGs, and establishing new SIGs and interagency groups (IGs). Meanwhile, in June 1982, Haig resigned and was replaced by George P. Schultz, signaling a move to a less activist State Department—even as the influence of the NSC continually increased.

**Iran-Contra and the fallout.** Robert McFarlane, with Admiral John Poindexter as his deputy, replaced Clark as National Security Advisor in October 1983. By then, the ever-growing number of committees had created an NSC bureaucracy that, critics would later charge, made it easy for Lieutenant Colonel Oliver North to carve out his own miniature empire within the NSC. More significant, however, was the fact that the NSC under McFarlane took an increasingly active role in formulating and implementing policy, particularly in the Middle East and Central America.

All these threads came together in the Iran-Contra situation, whereby the NSC (Poindexter replaced McFarlane as advisor in December 1985) sought to purchase the release of hostages held by pro-Iran groups in the Middle East and simultaneously provide funds to the Contras, anticommunist guerrillas in Nicaragua. They would do this by selling arms to the Iranian regime, which they believed they could cultivate as an ally against a common enemy, the Soviets. Arms sales would fund the Contras, to whom a Democrat-dominated Congress had refused support.

Once word of the Iran-Contra operation leaked to the press in late 1986, it sparked a scandal that would darken the remainder of Reagan's administration. In the wake of Iran-Contra, the Presidential Review Board—better known as the Tower Board after its leader, Senator John Tower—made a number of recommendations that collectively limited the size and power of the NSC.

In November 1986, Reagan appointed Frank Carlucci as National Security Advisor, with Lieutenant General Colin Powell as his deputy. Carlucci, whose tenure was marked by continued reforms of the NSC, served for less than a year before succeeding Caspar Weinberger as Secretary of Defense. Reagan replaced him with Powell, who ran an NSC that was tightly controlled, disciplined, efficient, and unobtrusive.

Vice President George Bush, elected to succeed Reagan, assumed office in January 1989, on the brink of momentous changes in the world. The Cold War was coming to an end, and the period that followed would give



rise to an increasingly uncertain international situation in which the United States would become involved in conflicts around the globe, including Panama in 1989, Kuwait in 1991, and Somalia in 1993.

In line with these changes, Bush altered the NSC. Colin Powell became Chairman of the JCS, while Scowcroft returned to his old position as National Security Advisor. This time, Scowcroft would hold more power than in the Kissinger years, and he enjoyed a close working relationship with the president. At the same time, Scowcroft helped sow friendly relations between the NSC and its old rival, the Department of State. Instead of constituting competing fiefdoms, the NSC, along with the State and Defense Departments and other key centers of power, more closely followed its original mandate of serving the administration's larger needs.

## The Clinton Era (1993–2001)

As had been the practice from Carter's time, William J. Clinton initiated his presidency with a presidential directive. Also like Carter and all presidents since, he created new names for his directives—Clinton's were called Presidential Decision Directives (PDD), for instance, in contrast to the National Security Directives of his predecessor—as well as for other aspects of NSC operations. PDD 1, for instance, issued on his first day in office, established these new names, while PDD 2 on the following day increased the membership of the NSC.

Thenceforth, in addition to the four statutory members (president, vice president, secretaries of State and Defense), members would include the secretary of the Treasury, the U.S. Representative to the United Nations, the Assistant to the President for National Security Affairs (i.e., the National Security Advisor), the Chief of Staff to the President, and the Assistant to the President for National Economic Policy. (The last, head of the newly created National Economic Council, was a creation of the Clinton administration.) DCI and the Chairman of the JCS would retain their statutory roles as advisors, while the Attorney General and others would attend when invited to do so.

## George W. Bush and the Post September 11, 2001, World (2001–present)

When George W. Bush assumed the presidency, he appointed Dr. Condoleezza Rice, most recently the provost of Stanford University, as his National Security Advisor. He also scaled back the roster of NSC members to the statutory core, with others invited to participate as needed. Eight months later, Bush's administrative agenda changed, along with the entire fabric of American life, in the aftermath of the September 11, 2001, terrorist attacks.

From at least the time of the 1993 terrorist attack on the World Trade Center towers, the Clinton administration

had declared a "war on terror," but until the attacks that brought those towers down eight years later, the "war" was ill-defined. With the launch of an attack against Afghanistan on October 7, 2001, the war became far more than a figure of speech. By that point, Americans had become accustomed to seeing Bush at public appearances surrounded by the other principal leaders in that war: Rice, Secretary of Defense Donald Rumsfeld, and Powell, now serving as Secretary of State.

Others sometimes appeared alongside this core group, among them one who most clearly qualified as a core participant: Vice President Dick Cheney. Like Rumsfeld and Powell, Cheney had served in past Republican administrations—in his case, that of Bush's father—but despite a close relationship, Bush and Cheney appeared together only infrequently to reinforce the idea that if anything happened to one leader, the other would be on hand to run the nation.

One figure identified with the core group was former Pennsylvania Governor Tom Ridge, leader of the newest Cabinet department, Homeland Security. By the late fall of 2001, there was already talk in policy circles about the return of the kind of turf battles that had animated the corridors of the White House decades earlier. Only the players had changed, and this time it was the NSC and the Office of Homeland Security (as it was known prior to March 2003) bickering over control of the White House Situation Room.

Battles of this kind will probably continue in one form or another for as long as the national leadership exists, and to an extent, they play a role in maintaining healthy checks and balances within a constitutional, democratic state possessing multiple centers of power. Conversely, it was emblematic of the post-September 11 America that the Bush team could act as much in concert with one another as they did. In a White House that had seen half a century's worth of struggles between the NSC and the Departments of State and Defense, the sight of Rice, Powell, and Rumsfeld standing shoulder-to-shoulder—not just literally but figuratively—was a testament to the sense of shared duty that animated many Americans in the early twenty-first century.

### ■ FURTHER READING:

#### BOOKS:

- Best, Richard A. *The National Security Council: An Organizational Assessment*. Huntington, NY: Novinka Books, 2001.
- Kissinger, Henry, and Clare Boothe Luce. *White House Years*. Boston: Little, Brown, 1979.
- Menges, Constantine Christopher. *Inside the National Security Council: The True Story of the Making and Unmaking of Reagan's Foreign Policy*. New York: Simon and Schuster, 1988.
- Prados, John. *Keepers of the Keys: A History of the National Security Council from Truman to Bush*. New York: Morrow, 1991.

Zegart, Amy B. *Flawed by Design: The Evolution of the CIA, JCS, and NSC*. Stanford, CA: Stanford University Press, 1999.

#### PERIODICALS:

Newman, William W. "Reorganizing for National Security and Homeland Security." *Public Administration Review* 62 (September 2002): 126–137.

#### ELECTRONIC:

History of the National Security Council. American Federation of Scientists. <<http://www.fas.org/irp/offdocs/NSChistory.htm>> (March 24, 2003).

#### SEE ALSO

*Bush Administration (1989–1993), United States National Security Policy*  
*Bush Administration (2001–), United States National Security Policy*  
*Carter Administration (1977–1981), United States National Security Policy*  
*Clinton Administration (1993–2001), United States National Security Policy*  
*Department of State, United States*  
*Eisenhower Administration (1953–1961), United States National Security Policy*  
*Executive orders and Presidential directives*  
*Ford Administration (1974–1977), United States National Security Policy*  
*Johnson Administration (1963–1969), United States National Security Policy*  
*Kennedy Administration (1961–1963), United States National Security Policy*  
*National Security Act (1947)*  
*National Security Advisor, United States*  
*Nixon Administration (1969–1974), United States National Security Policy*  
*NSC (National Security Council)*  
*Reagan Administration (1981–1989), United States National Security Policy*  
*Truman Administration (1945–1953), United States National Security Policy*

---

## NSF (National Science Foundation)

---

The National Science Foundation (NSF) directs and funds science research. An independent agency in the United States government, the NSF was established May 10, 1950, by passage of the National Science Foundation Act. Subsequent amendments to the act granted the NSF further authority to develop, fund, and oversee research in the government, academic, and industrial sectors.

The stated mission of the National Science Foundation is to promote scientific research that aids national health and prosperity, and protects national security interests. The foundation endeavors to foster communication

and cooperation in the national and global science communities. A president-appointed director, deputy director, and eight assistant directors govern the agency. The foundation is further staffed by the twenty-four member National Science Board.

The NSF grants student fellowships for graduate studies in the sciences, medicine, and engineering, and sponsors post-doctoral research opportunities. Research programs backed by the NSF range in scope from disease research to space exploration. The foundation also develops science education programs for school-aged children, and cosponsors symposia, conferences, and seminars for college students and professional researchers. In conjunction with independent researchers, professional organizations, government agencies, and international scholars, the NSF publishes and revises a code of ethical research practices.

The NSF often works in conjunction with the Defense Advanced Research Projects Agency (DARPA), an organization within the Department of Defense, to develop research projects with military, intelligence, and national security interests. In 2001, the two organizations cosponsored research concerning government computer systems and data security. While NSF may aid research with implications on national security and military technology, DARPA is responsible for classified weapons and technology research.

As a response to the September 11, 2001, attacks on the United States, the NSF has increased its backing of scientific research beneficial to counterterrorism. Studying epidemic disease, combating the effects of biological and chemical weapons, water and soil safety, and developing better information protection systems are some of the present science- and engineering-related national security issues addressed by NSF sponsored research.

#### ■ FURTHER READING:

#### ELECTRONIC:

National Science Foundation. <<http://www.nsf.gov>> (15 January 2003).

#### SEE ALSO

*DARPA (Defense Advanced Research Projects Agency)*

---

## NTSB (National Transportation Safety Board)

---

The United States National Transportation Safety Board (NTSB) is an independent national agency responsible for investigating transportation accidents within the United States. The agency has custody of all debris and wreckage



Investigators from the National Transportation Safety Board (NTSB) gather around the wreckage of American Airlines flight 1420, which crashed June 1, 1999. ©AFP/CORBIS.

from accidents that it investigates, and thorough investigations sometimes take years to complete. The primary focus of NTSB operations is the investigation of civil aviation accidents, however the agency is also required to report on railroad, pipeline, and significant marine and highway accidents. For the NTSB to be involved in an accident investigation, the accident must involve a national transportation infrastructure, a public vessel, or hazardous materials.

The NTSB was established on April 1, 1967. In its early days, the agency worked closely with the Department of Transportation. Concerned with the NTSB's ties to the nation's transportation regulatory agency and the transportation industry, Congress sought to make the NTSB an independent, and impartial, entity. In 1975, the agency became independent, receiving funding in its own right through the Independent Safety Board Act.

The NTSB is managed by a five-person board. Members are appointed by the President to serve five-year terms. The board directs agency field investigators, and certifies final accident reports.

In addition to accident investigation, the NTSB maintains the government database of civil aviation accidents. The database permits NTSB researchers to search for patterns in accident occurrence, as well as publish safety statistics for carriers and airports. The NTSB conducts regular studies of transportation safety procedures, making improvement suggestions to transportation officials and Congress when necessary. Since its inception in 1967, the NTSB has issued nearly 12,000 recommendations. Though the NTSB does not have the power to act as a regulatory authority, most of its recommendations have been adopted by the national transportation industry.

The NTSB is also an instrument of national transportation law. The board sometimes hears the appeals of pilots, mechanics, and mariners who have been stripped of professional privileges, certificates, or incurred disciplinary fines. For advice on these cases, the NTSB employs legal council. Council is also provided to any witnesses or parties involved in an accident who are questioned by NTSB investigators.

Although the investigative jurisdiction of the NTSB does not extend beyond national borders, the agency

provides investigators for international accidents involving United States registered aircraft or maritime vessels. United States NTSB investigators, or foreign NTSB Accredited Representatives, have occasionally been welcomed by foreign governments that do not have their own investigative services to report on accidents.

After the 2001 terrorist attacks on the United States, the NTSB began widespread investigations of the airlines' safety and screening procedures. The newly created Transportation Safety Administration temporarily assumed many of the NTSB safety recommendation duties. The NTSB continues to investigate the actual September 11, 2001, airline crashes associated with the terrorist attacks.

#### ■ FURTHER READING :

##### ELECTRONIC:

United States National Transportation Safety Board. <<http://www.nts.gov>> (30 April 2003).

##### SEE ALSO

*Airline Security  
Aviation Security Screeners, United States  
FAA (United States Federal Aviation Administration)  
September 11 Terrorist Attacks on the United States*

---

## Nuclear Detection Devices

---

■ LARRY GILMAN

Nuclear detection devices, also termed radiation detectors, are systems designed to detect the presence of radioactive materials. These materials may take the form of gases, particles suspended in air, or solid metals (often alloys of uranium or plutonium). Detection of nuclear materials is needed for safety monitoring of all facilities handling nuclear materials, for the interdiction of nuclear smuggling, and for arms-control monitoring of peaceful nuclear programs to detect any diversions of fissile material to bomb-building programs.

Although radioactive materials can be (and, in the laboratory, often are) detected by direct chemical assay, it is far easier in practice to detect them at second hand by measuring the radiation they emit. Nuclear materials emit two kinds of radiation as the nuclei of their atoms spontaneously break apart: fast particles (i.e., neutrons, electrons, and ions) and electromagnetic radiation (i.e., X rays and gamma rays). Different nuclear materials emit different blends of these radiation types. This radiation, unless blocked by layers of matter (shielding), reveals the presence of the nuclear material. The use of nuclear detection devices or radiation detectors is thus, key to monitoring

for the presence of radioactive substances. The arms-control monitoring programs of the International Atomic Energy Agency, for example, depend heavily on both automated and hand-carried detection devices that seek to measure the telltale radiations emitted by nuclear materials.

Furthermore, radiation can cause illness, injury, or death. A single fast particle, X ray, or gamma ray can damage a DNA molecule so that a healthy cell is converted to a cancer cell, and sufficiently large numbers of particles or rays can disturb enough of a cells' molecules to kill it. Therefore, nuclear detection devices are also used to alert to releases of radioactive material, whether deliberate (e.g., caused by a "dirty bomb") or accidental (e.g., material escaping from a nuclear power plant, waste-storage facility, or fuel-reprocessing plant).

To be detectable, radiation must be partly or wholly absorbed by ordinary matter. Radiation is said to have been absorbed by a mass of material when it has given up most or all of its energy to that material; radiation that is difficult to absorb (e.g., neutrino flow) is correspondingly difficult to detect. There are several different radiation-absorption phenomena, each of which is exploited in the design of a different class of detection devices. The most important form of absorption is ionization, that is, the separation of neutral atoms in the absorbing medium into free electrons (negatively charged) and free ions (positively charged atoms lacking one or more electrons). All forms of radiation mentioned above can cause ionization. Ionization, in turn, can be detected in numerous ways. One way is chemical, as ions, because they lack electrons, readily combine with other atoms to form new molecules. In a photographic film, this recombination appears as the chemical change known as exposure. Film-badge dosimeters measure radiation by accumulating chemical changes in response to ionizing radiation.

A more precise and continuous measure of ionizing radiation is obtained by electronic amplification of individual ionization events. The best known of the tools that measures radiation in this way is the Geiger counter. In a Geiger counter, a voltage is placed across a chamber filled with gas (usually argon or xenon); this causes an electric field to exist between one end of the chamber and the other. When a fast particle or high-energy ray passes through the chamber, it ionizes neutral atoms, that is, splits them up into free electrons and positively-charged ions. Under the influence of the electric field, the electrons accelerate toward one end of the chamber and the ions toward the other. If the electrical field is strong enough, it accelerates them enough so that when they strike other atoms in the gas they ionize them as well. The electrons and ions thus produced may also be accelerated enough to cause ionization, and so on. The resulting brief avalanche of charged particles constitutes a pulse of electrical current that can be detected, amplified, and counted by appropriate circuitry. In the audio output circuit of a Geiger counter, a single ionization event is amplified to produce the device's trademark "click." Although the arrival



A Nuclear Emergency Search Team (NEST) member shows portable sensing equipment used to detect radioactive sources. The briefcase design allows NEST members to carry the sensing device undetected in crowded environments. AP/WIDE WORLD PHOTOS.

of any one ray or particle is a randomly timed event, the average rate of such arrivals, smoothed over time, gives an accurate idea of how much radiation is present.

Another type of radiation-detection device is the scintillation detector. Certain crystals, when struck by a single high-energy photon or particle, produce a scintillation, that is, a flash of light consisting of thousands or tens of thousands of visible photons. In the early twentieth century, one method of measuring radiation was to count scintillation rates under a microscope; modern detectors use electronic circuits for the same purpose.

The interactions of radiation with semiconducting crystals such as silicon can also be measured. Semiconducting radiation detectors have the advantages of small size, high sensitivity, and high accuracy.

#### ■ FURTHER READING:

##### BOOKS:

Delaney, C. F. G., and E. C. Finch. *Radiation Detectors*. New York: Oxford University Press, 1992.

##### SEE ALSO

*Dosimetry*

## Nuclear Emergency Support Team, United States

The Nuclear Emergency Support Team (NEST) is part of an emergency response branch of the National Nuclear Security Administration (NNSA), itself a unit of the United States Department of Energy (DOE). Established in the mid-1970s—long before NNSA itself—NEST has analyzed hundreds of cases involving potential nuclear threats. It is one of seven emergency response groups operated by NNSA, and members work in the field alongside the Federal Bureau of Investigation's Domestic Emergency Support Team or the State Department's Foreign Emergency Support Team.

**NEST in the NNSA emergency response context.** The seven NNSA emergency response teams include the Aerial Measuring System, which detects, measures, and tracks radioactive material; the Atmospheric Release Advisory Capability, which monitors and predicts the release of hazardous materials into the atmosphere; the Accident Response Group, which supports the successful resolution of U.S. nuclear weapons accidents anywhere in the world; the



Nuclear Emergency Search Team members install radiation-sensing equipment into a helicopter at the NEST facility at Nellis Air Force Base in Nevada. AP/WIDE WORLD PHOTOS.

Federal Radiological Monitoring and Assessment Center, which coordinates radiological efforts on the federal, state, and local levels; the Radiological Assistance Program, the usual NNSA first responder in radiological emergencies; the Radiation Emergency Assistance Center/Training Site, which trains respondents and provides medical treatment for injuries resulting from radiation exposure; and NEST, which provides specialized technical expertise in response to nuclear or radiological terrorist incidents.

Established in 1975, NEST has addressed a variety of possible nuclear threats. For example, in its first year of operation, NEST responded to a threat by a group claiming that it would detonate a nuclear device in New York City if it were not given \$30 million. Police provided what was purportedly a payment, but actually a lure for the criminals, who failed to materialize—along with their alleged bomb. NEST has analyzed the credibility of some 60 extortion threats involving nuclear materials, 25 reactor threats, and 20 non-nuclear extortion threats. It has also investigated well over 650 reports of illegal sales involving nuclear materials.

**NEST at work.** As of the early twenty-first century, NEST had some 70 responders and a larger pool of approximately 900 personnel on call. Operational teams of 45 or fewer

people, including chemists, physicists, mathematicians, communications specialists, and technicians, are equipped with handheld detectors. In addition to four helicopters and three planes, they have vans fitted with detectors and diagnostic equipment. A support department even supplies fake commercial artwork to disguise NEST vans.

Not surprisingly, NEST's services have been in particularly high demand since September 11, 2001. In January 2002, the administration of President George W. Bush called on NEST to search large U.S. cities for a possible "dirty bomb"—a crude nuclear device—that was a reported tool of the terrorist organization al Qaeda. NEST teams, equipped with gamma and neutron detectors, could blend into crowds by disguising their equipment as briefcases, backpacks, or even beer coolers. In February, 2002, NEST teams also quietly provided support to security efforts at the Winter Olympics in Salt Lake City, Utah.

#### ■ FURTHER READING:

##### PERIODICALS:

Hall, Mimi. "Preparations Underway for Radiation Attack." *USA Today*. (July 8, 2002): A2.

Waller, Douglas. "The Secret Bomb Squad." *Time*. (March 18, 2002): 23.

## ELECTRONIC:

National Nuclear Security Administration. <<http://www.nnsa.doe.gov>> (March 7, 2003).

Oppenheimer, Andy. Nuclear Incident Response in the U.S. *Jane's International Security News*. <[http://www.janes.com/security/international\\_security/news/jcbw/jcbw020827\\_1\\_n.shtml](http://www.janes.com/security/international_security/news/jcbw/jcbw020827_1_n.shtml)> (March 26, 2003).

Render Safe, Defusing a Nuclear Emergency. Los Alamos National Laboratory. Fall 2002. <[http://www.lanl.gov/quarterly/q\\_fall02/render\\_safe.shtml](http://www.lanl.gov/quarterly/q_fall02/render_safe.shtml)> (March 26, 2003).

## SEE ALSO

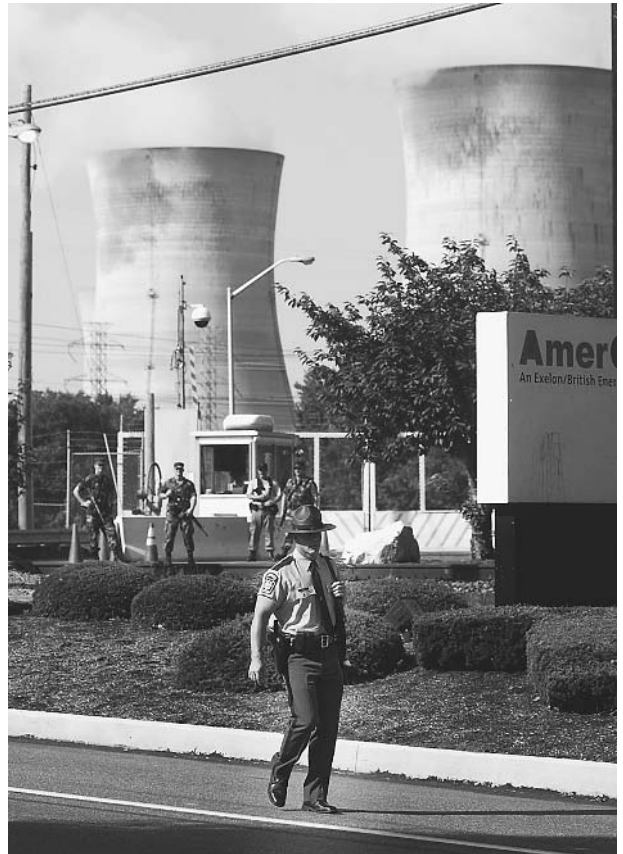
*Atmospheric Release Advisory Capability (ARAC)*  
*Domestic Emergency Support Team, United States*  
*FEST (United States Foreign Emergency Support Team)*  
*NNSA (United States National Nuclear Security Administration)*  
*Radiological Emergency Response Plan, United States Federal*

## Nuclear Power Plants, Security

■ LARRY GILMAN

Nuclear power plants pose two basic security concerns. First, all nuclear reactors both use and produce radioactive elements (e.g., uranium and plutonium) that can be used to build nuclear weapons. Second, all reactors and nuclear-waste storage facilities contain large amounts of radioactive material. This material might be stolen for later use as a terrorist weapon (e.g., by being combined with conventional explosives to form a radiological dispersal weapon, also termed a "dirty bomb") or, in the case of concentrated fuel, to build nuclear weapons. Alternatively, radioactivity might be released directly to the environment by sabotaging safety systems or blowing up a facility with missiles, planted charges, or hijacked jet aircraft. Thus, nuclear facilities on a nation's own territory threaten its security as a target of enemy action, while nuclear facilities on an enemy's territory threaten security as a possible source of nuclear weapons.

Nuclear proliferation, as the possession of nuclear weapons by ever-greater numbers of nations is termed, has been a recognized global hazard since at least the 1960s. In contrast, the possibility that nuclear facilities on one's own territory might be employed by an enemy as ready-made weapons has been of greatly heightened public concern since the terror attacks of September 11, 2001. Both threats are serious and plausible. Even a relatively small nuclear weapon of the size that destroyed the city of Hiroshima on August 9, 1945, could kill hundreds of thousands of people, and such a bomb requires only



A Pennsylvania State Police officer patrols the entrance of the Three Mile Island nuclear power plant near Harrisburg, Pennsylvania, in July 2002, as security at power plants has been increased since the attacks of September 11, 2001. AP/WIDE WORLD PHOTOS.

about 15 lb (7 kg) of uranium-235 ( $U^{235}$ ) or a similar quantity of plutonium. Every large (i.e., 100-MW range) nuclear power plant contains hundreds of pounds of both these substances and produces hundreds of additional pounds of plutonium every year. Meanwhile, release of a significant fraction of the radioactive material in any large nuclear reactor, reprocessing plant, or waste-storage facility could cause an unpredictable number of deaths over a continent-sized area and make thousands of square miles of land uninhabitable for time periods ranging from days to centuries.

**Reactor fuel and bomb material.** Both nuclear reactors and fission-type nuclear weapons exploit the fact that atoms of some elements (e.g., uranium and plutonium) are unstable, that is, their nuclei have a natural tendency to break apart. When a nucleus breaks apart (fissions), it releases smaller nuclei, electrons, high-energy photons, and fast-moving neutrons. If one of these neutrons strikes another unstable nucleus, that nucleus may also fission, releasing still more neutrons, which may trigger still other nuclei, and so on and so on in a self-sustaining chain reaction. This chain reaction is the energy source of both reactors

and fission bombs, the main difference being that in a reactor the chain reaction proceeds at approximately constant speed, while in a bomb, it spreads at geometrically increasing speeds.

Reactor fuel—the mixture of radioactive metals used to sustain a chain reaction in the core of a typical electricity-generating reactor—is only 3–5 percent  $U^{235}$ , the rest being mostly uranium-238 ( $U^{238}$ ), a comparatively stable form of uranium. This means that a nuclear bomb cannot be made directly out of ordinary commercial reactor fuel. However, “research” reactors, most of which produce radioisotopes for medical and industrial purposes, run on nearly pure  $U^{235}$ , the same material used to destroy Hiroshima. There are about 550 such reactors in the world, several of which—including Israel’s reactor at Dimona—have actually been used to produce nuclear weapons clandestinely. Furthermore, during the ordinary process of “burning” reactor fuel some of its  $U^{238}$  is changed by neutron bombardment to plutonium-239 ( $Pu^{239}$ ). This can be extracted from the spent fuel, concentrated, and used either as reactor fuel or to build bombs.

Western intelligence sources assume that India, Israel, Pakistan, South Africa, and (probably) North Korea have built nuclear weapons using  $U^{235}$  or  $Pu^{239}$  obtained from reactor programs publicly dedicated to research or electrical power generation. Other nations will probably do so in the future.

**Security and proliferation.** For many years, as part of the Atoms for Peace program initiated by President Eisenhower in 1953, the United States literally gave away reactors, nuclear materials, and essential nuclear knowledge to many countries. At least 26 reactors fueled by highly-enriched (bomb-grade) uranium were given to countries including Argentina, Brazil, Iran, Israel, South Korea, Pakistan, Spain, and Taiwan. Thousands of scientists from these countries and others were trained in reactor theory, plutonium extraction and enrichment, and other knowledge essential to nuclear bomb manufacture. Thanks to Atoms for Peace (and sales of nuclear technologies by other nuclear powers), preventing the global proliferation of nuclear weapons by restricting nuclear materials, reactors, and reprocessing facilities to a relatively few states ceased to be an option long ago. Nuclear proliferation has occurred and will probably continue. Israel is now believed by most observers to possess more than 200 nuclear weapons, India exploded its first nuclear weapon in 1974, and Pakistan (whose first nuclear reactor was a gift from the U.S.) exploded its first nuclear weapon in 1998.

Systematic efforts, however, have been made to control the proliferation of nuclear weapons worldwide. The International Atomic Energy Agency (IAEA) is an arm of the United Nations charged with the promotion and global monitoring of nuclear power. The IAEA has sought, through inspections programs, to prevent the diversion of nuclear materials from reactors to weapons. Compliance with

IAEA inspections is, however, voluntary. Furthermore, diversions below the “measurement noise level” could suffice to build a nuclear weapon. For example, in a nuclear facility where 1,000 1-kilogram units of fissionable material were measured to an accuracy of .001 kilogram each year, up to 1 kilogram (1,000 samples of less than .001 kg each) could be undetectably diverted annually, and enough for a bomb accumulated in a few years. Many observers deem it unlikely that any state seriously desiring to manufacture nuclear weapons has yet been prevented from doing so by IAEA inspections.

Another method for controlling proliferation, so far adopted only by Iran and Israel, is the destruction of nuclear facilities possessed by enemy states. On September 30, 1980, planes bearing Iranian markings destroyed Iraq’s Tuwaitha nuclear research center near Baghdad, the capital of Iraq. On June 7, 1981, 16 Israeli aircraft destroyed the Osirak “research” reactor just south of Baghdad. Israel had tried to prevent completion of the French-supplied facility by means of threatening letters, sabotage, and assassination, but had failed. (The June 7 air attack demolished the facility before it was fueled and operational, so no life-threatening release of radiation occurred.) These attacks may have been effective in their goal of preventing Iraq from obtaining nuclear weapons. However, it is not practical to prevent nuclear proliferation by these means on a global scale.

Thus there does not seem to be any long-term, sure-fire method of preventing technically sophisticated countries that possess nuclear reactors from exploiting them to build nuclear weapons if they so desire. If this is true, absolute security from nuclear weapons is a chimerical goal, and the best that can be hoped for is ongoing negotiation for a state of permanent, radical, and global *insecurity*.

**Protecting nuclear facilities.** Many radioactive elements besides  $Pu^{239}$  accumulate in reactor fuel as it is irradiated in a reactor core. The fast-moving particles and high-energy photons emitted by these elements can kill living things either directly or by causing genetic damage; spent reactor fuel and materials derived from it are, therefore, dangerous to approach or ingest. Furthermore, they will remain so for periods of time greatly exceeding the duration of human history thus far;  $Pu^{239}$ , for example, has a half-life of approximately 24,000 years (i.e., only half the atoms in any sample of  $Pu^{239}$  will have fissioned after 24,000 years).

Material radioactive enough to be classified as high-level waste is produced continuously by operating nuclear reactors and by facilities that reprocess spent fuel to extract plutonium. For example, the fuel in a typical electricity-generating reactor (of which 104 are operating in the United States) must be swapped out for fresh fuel every few years. The best long-term hope for disposing of this spent fuel is deep burial in rocks that seem likely to



remain stable for hundreds of thousands of years. However, in most of the world, including the United States, no deep-burial program yet exists, so all high-level waste is stored on the surface in containers, usually on the grounds of the nuclear plants that produce it. Release to the environment of the material in even one such repository would be a highly effective act of terrorism.

Persons wishing to attack a nuclear reactor or other nuclear facility have a wide range of options. They may seek to intercept or sabotage shipments of fuel or waste; invade a facility using armed force or deception, then proceed to steal radioactive material, blow up the facility, or (if it is a reactor) cause it to melt down; or seek to breach the containments of reactors or waste-storage facilities using truck bombs, missiles, hijacked aircraft, or other means. All facilities containing significant amounts of radioactive material must therefore be defended from a wide range of possible attacks.

Reactor and waste-storage security has been based for decades on a concept termed "defense in depth." The defense-in-depth method requires that each nuclear facility be surrounded by concentric security barriers. The outermost barrier is invariably a high fence topped with razorwire. The grounds near the fence, inside and out, are monitored by intruder-detection devices, and vehicles can only enter through checkpoints staffed by armed guards. Thirty to 40 guards are on duty at all times at a typical nuclear power plant, and vehicle gates, doors, and the like remain locked.

Defense in depth seeks to provide security against an imaginary scenario termed the Design Basis Threat, which is defined by the U.S. Nuclear Regulatory Commission (NRC). Prior to September 11, 2001, the Design Basis Threat included a truck bomb the size of that used to attack the World Trade Center in 1993, three outside attackers, and one collaborator inside the plant. Also, the NRC stated in its public-relations material that there was no credible security threat to the nation's nuclear facilities. The NRC removed these statements from the Web along with the rest of its website shortly after the September attacks, wishing to "review posted material to make sure there was no sensitive information that could be misused to harm the security of our nation" (<http://www.nrc.gov/what-we-do/safeguards/response-911.html>).

However, among some scientists, there had long been skepticism about the adequacy of defense in depth and the Design Basis Threat. From the 1970s until 2001, the NRC staged mock attacks (termed Operational Safeguard Response Evaluations) to test plant security. Forty-six percent of plants tested from the 1970s until 1998 failed evaluation; from 1998 to September 11, 2001, 9 out of 11 plants tested failed; no evaluations have been conducted since. Furthermore, doubts linger about the ability of plant personnel to defend against determined attack. Most of the guards who are supposed to be able to repel a determined (perhaps suicidal) paramilitary or terrorist assault are actually hired from private security companies, in

some cases paid less than janitors working at the same facilities. In the wake of the September 11, 2001 attacks, state troopers and National Guard troops have been deployed to assist these personnel in guarding nuclear plants against attack; however, in response to NRC orders to increase security, some are now working extraordinarily long hours, and further supplemental plans are under review.

The terrorist attacks of September 2001 have given official credibility to the use of wide-body civilian aircraft as weapons. However, no nuclear facility has been specifically designed to withstand such an attack. The NRC states that "previously...[it] had no reason to perform a detailed engineering analysis of the consequences of a deliberate attack on nuclear facilities by a large airliner," yet the idea of targeting reactors with jumbo jets was being pointed out over twenty years ago by critics who recalled the Christmas Day, 1974, hijacking of a jumbo jet by a man who threatened to crash it into the center of Rome. (The man was overpowered after making his threat.) It is likely that such extreme threats to nuclear-facility security were not considered prior to September 11 not because nobody had thought of them but because (a) they were thought to be highly improbable, and (b) the cost of rendering facilities attack-proof against them (e.g., by building them underground) would have made nuclear power too expensive to develop for civilian markets.

The NRC states that it is now analyzing the consequences of an aerial attack on a nuclear power plant and plans to upgrade its Design Basis Threat to include as many attackers as were involved in the attacks of September 2001. It is not known whether the new NRC standard, when announced, will include provisions for defending plants against jumbo jets used as weapons, either by shooting them down or hardening reactor facilities against massive impact and fire. It is also not known what security precautions the NRC will mandate for in-transit nuclear waste if the federally-owned deep-storage facility at Yucca Mountain, Nevada, begins to receive high-level waste shipments from around the country in 2010 as planned.

As of July 2002, at least 16 states had taken the precaution of requesting stockpiles of potassium iodide pills from the NRC. All persons, especially children, are vulnerable to thyroid cancer caused by even small quantities of radioactive iodine, a substance expected to be a major component of the fallout from any nuclear incident. If ingested in a timely way, potassium iodide saturates the thyroid gland with non-radioactive iodine and prevents it from absorbing lethal levels of radioactive isotopes.

**Conclusion.** The security of nuclear facilities of all kinds is under more intense scrutiny—both by defenders and by potential attackers—than ever before, and not only in the United States. Old security standards are now admitted to have been inadequate, but enhanced standards have not yet been officially defined and uniformly implemented.

The goal of security—both from nuclear weapons derived from power plants and other “peaceful” facilities, and from takeover of nuclear facilities by groups of well-armed attackers—remains urgent, but elusive. In January 2002, President George W. Bush announced that “diagrams of nuclear power plants” had been found among items captured from terrorist groups in Afghanistan.

#### ■ FURTHER READING:

##### BOOKS:

Lovins, Amory B., and L. Hunter Lovins. *Brittle Power: Energy Strategy for National Security*. Andover, MA: Brick House Publishing, 1982.

———. *Energy/War: Breaking the Nuclear Link*. San Francisco: Friends of the Earth, 1980.

Ramberg, Bennett. *Nuclear Power Plants as Weapons for the Enemy: An Unrecognized Military Peril*. Berkeley, CA: University of California Press, 1984.

##### PERIODICALS:

Wald, Matthew L. “Guards at Nuclear Plants Say They Feel Swamped by a Deluge of Overtime.” *New York Times*. October 20, 2002.

##### ELECTRONIC:

“States Mull Anti-Cancer Pill in Response to Terrorist Attack.” National Council of State Legislatures. July, 2002. <<http://www.ncsl.org/programs/health/anticancerpills.htm>> (December 11, 2002).

“Nuclear Security—Before and After September 11.” U.S. Nuclear Regulatory Commission. September 23, 2002. <<http://www.nrc.gov/what-we-do/safeguards/response-911.html>> (December 11, 2002).

##### SEE ALSO

*Nuclear Regulatory Commission (NRC), United States Weapon-Grade Plutonium and Uranium, Tracking*

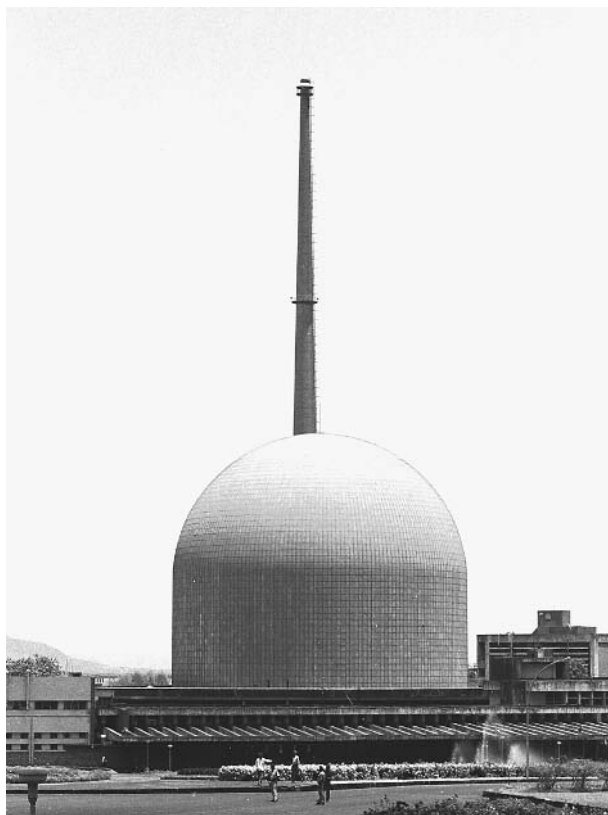
## Nuclear Proliferation.

SEE *Non-Proliferation and National Security, United States*.

## Nuclear Reactors

#### ■ LARRY GILMAN

Nuclear reactors are complex devices in which fissionable elements such as uranium, thorium, or plutonium are made to undergo a sustainable nuclear chain reaction.



Nuclear reactor at the Bhabha Atomic Research Center in Bombay, photographed in 1997, near the site of a unit that extracted plutonium for use in India's 1974 nuclear tests. AP/WIDE WORLD PHOTOS.

This chain reaction releases energy in the form of radiation that (a) sustains the chain reaction; (b) transmutes (i.e., alters the nuclear characteristics of) nearby atoms, including the nuclear fuel itself; and (c) may be harvested as heat. Transmutation in nuclear reactors of the common but weakly fissionable nuclide uranium-238 ( $^{238}\text{U}$ ) into plutonium-239 ( $^{239}\text{Pu}$ ) is an important source of explosive material for nuclear weapons, and heat from nuclear reactors is used to generate approximately 16 percent of the world's electricity and to propel submarines, aircraft carriers, and some other military vessels. Nuclear reactors have also been used on satellites and proposed as power sources for locomotives, aircraft, and rockets.

**How a nuclear reactor works.** A nuclear reactor exploits the innate instability of some atoms—in general, those that have a large atomic number or that contain an imbalance of protons and neutrons—which break apart (fission) at random times, releasing photons, neutrons, electrons, and alpha particles. For some nuclides (atomic species having a specific number of protons and neutrons in the nucleus), the average wait until a given atom spontaneously fissions is shorter. When enough atoms of such an unstable isotope are packed close together, the neutrons released by fissioning atoms are more likely to strike the

nuclei of nearby unstable atoms. These may fission at once, releasing still more neutrons, which may trigger still other fission events, and so forth. This is the chain reaction on which nuclear reactors and fission-type nuclear bombs depend. In a reactor, however, the fission rate is approximately constant, whereas in a bomb it grows exponentially, consuming most of the fissionable material in a small fraction of a second.

To produce a sustained chain reaction rather than a nuclear explosion, a reactor must not pack its fissionable atoms too closely together. They are therefore mixed with less-fissionable atoms that do not sustain the chain reaction. For example, in a reactor utilizing  $^{235}\text{U}$  as its primary fuel, only 3 percent of the fuel is actually  $^{235}\text{U}$ ; the rest is mostly  $^{238}\text{U}$ , a much less fissionable isotope of uranium. The higher the ratio of active fuel atoms to inert atoms in a given fuel mix, the more "enriched" the fuel is said to be; commercial nuclear power plant fuel is enriched only 3 to 5 percent  $^{235}\text{U}$ , and so cannot explode. For a fission bomb, 90 percent enrichment would be typical (although bombs could be made with less-enriched uranium). Naval nuclear reactors, discussed further below, have used fuels enriched to between 20 and 93 percent.

Having diluted its active fuel component (e.g.,  $^{235}\text{U}$ ), a typical nuclear reactor must compensate by assuring that the neutrons produced by this diluted fuel can keep the chain reaction going. This is done, in most reactors, by embedding the fuel as small chunks or "fuel elements" in a matrix of a material termed a "moderator." The moderator's function is to slow (moderate) neutrons emitted by fissioning atoms in the fuel. Paradoxically, a slow neutron is more likely to trigger fission in a uranium, plutonium, or thorium nucleus than a fast neutron; a moderator, by slowing most neutrons before allowing them to strike nuclei, thus increases the probability that each neutron will contribute to sustaining the chain reaction. Graphite (a form of pure carbon), water, heavy water (deuterium dioxide or  $^2\text{H}_2\text{O}$ ), and zirconium hydride can all be used as moderators. Ordinary water is the most commonly used moderator.

If the chain reaction sustained by a nuclear reactor produces enough heat to damage the reactor itself, that heat must be carried off constantly by a gas or liquid as long as the reactor is operating. Once removed from the reactor, this energy may be ejected into the environment as waste heat or used, in part, to generate electricity. (Electricity, if generated, is an intermediate energy form; all the energy generated in a nuclear reactor or other power plant eventually winds up in the environment as heat.) In the case of a nuclear-powered rocket, such as the one the U.S. National Aeronautics and Space Administration (NASA) seeks to develop with its Project Phoenix, heat is removed from the system by ejected propellant. Liquid sodium, pressurized water, boiling water, and helium have all been used as cooling media for nuclear reactors, with pressurized or boiling water being used by commercial nuclear power plants. Typically, heat energy

removed from the reactor is first turned into kinetic energy by using hot gas or water vapor to drive turbines (essentially enclosed, high-speed windmills), then into electrical energy by using the turbines to turn generators.

Nuclear power sources that do not produce enough heat to melt themselves, and which therefore require no circulating coolant, have been used on some space probes and satellites, both U.S. and Russian. Such a power source, termed a radioactive thermoelectric generator or RTG, consists of a mass of highly radioactive material, usually plutonium, that radiates enough heat to allow the generation of a modest but steady flow of electricity via the thermoelectric effect. The efficiency of an RTG is low but its reliability is very high.

**Reactor byproducts.** The neutron flow inside a reactor bombards, and by bombarding changes, the nuclei of many atoms in the reactor. The longer a unit of nuclear fuel remains in a reactor, therefore, the more altered nuclei it contains. Most of the new atoms formed are radioactive nuclides such as cesium-144 or ruthenium-106; a significant number are, if  $^{238}\text{U}$  is present, isotopes of plutonium, mostly  $^{239}\text{Pu}$ . (Absorption of one neutron by a  $^{238}\text{U}$  nucleus turns it into a  $^{239}\text{Pu}$  nucleus; absorption of one, two, or three neutrons by a  $^{239}\text{Pu}$  nucleus turns it into a  $^{240}\text{Pu}$ ,  $^{241}\text{Pu}$ , or  $^{242}\text{Pu}$  nucleus.) Plutonium is found in nature only in trace amounts, but is present in all spent nuclear fuel containing  $^{238}\text{U}$ . If it is extracted for use as a reactor fuel or a bomb material, it is considered a useful by-product of the nuclear reactor; otherwise, it is a waste product. In either case, plutonium is highly toxic and radioactive, and remains so for tens of thousands of years unless it is further transmuted by particle bombardment, as in a particle accelerator, reactor, or nuclear explosion. Reactors specially designed to turn otherwise inert  $^{238}\text{U}$  into  $^{239}\text{Pu}$  by neutron bombardment are termed fast breeder reactors, and can produce more nuclear fuel than they consume; however, all nuclear reactors, whether designed to "breed" or not, produce plutonium.

This fact has a basic military consequence: Every nation that possesses a nuclear power plant produces plutonium, which can be used to build atomic bombs. Plutonium sufficiently pure to be used in a bomb is termed bomb-grade or weapons-grade plutonium, and the process of extracting plutonium from irradiated nuclear fuel is termed reprocessing. (The alloy used in sophisticated nuclear weapons is nearly pure plutonium, but the U.S. Department of Energy has estimated that an unwieldy bomb could be made with material that is only 15 to 25 percent plutonium, with less-unwieldy bombs being possible with more-enriched alloys.) Every nation that possesses a nuclear reactor and reprocessing capability thus possesses most of what it needs to build nuclear weapons. Several nations, including India and Pakistan, have in fact built nuclear weapons using plutonium reprocessed from "peaceful" nuclear-reactor programs. A large (100 MW electric) nuclear power plant produces enough plutonium for several dozen bombs a year.

Besides producing plutonium that can, and sometimes is, extracted to produce nuclear weapons, every nuclear reactor has the feature that if bombed, its radioactive contents could be released into the environment, greatly amplifying the destructive effects of a wartime or terrorist attack. Nuclear reactors thus have a two-edged aspect: as producers, potentially, of weapons for use *against* an enemy, and as weapons, if attacked, *for* an enemy.

**Naval nuclear reactors.** The primary military use of nuclear reactors, apart from the production of material for nuclear weapons, is the propulsion of naval vessels. Nuclear power sources enable naval vessels to remain at sea for long periods without refueling; modern replacement cores for aircraft carriers are designed to last at least 50 years without refueling, while those for submarines are designed to last 30 to 40 years. In the case of submarines, nuclear power also makes it possible to remain submerged for months at a time without having to surface for oxygen. Furthermore, reactors have the general design advantage of high power density, that is, they provide high power output while consuming relatively little shipboard space. A large nuclear-powered vessel may be propelled by more than one reactor; the U.S. aircraft carrier USS *Enterprise*, launched in 1960, is powered by eight reactors. Britain, France, China, and Russia (formerly the Soviet Union) have also built nuclear-powered submarines and other vessels.

Although the design details of the nuclear reactors used on submarines and aircraft carriers are secret, they are known to differ in several ways from the large land-based reactors typically used for generating electricity. The primary difference is that in order to achieve high power density, naval reactors use more-highly-enriched fuel. Older designs used uranium enriched to at least 93 percent <sup>235</sup>U; later Western reactors have used uranium enriched to only 20 to 25 percent, while Russian reactors have used fuels enriched to up to 45 percent. Small quantities of ex-Soviet submarine fuel have appeared on the global black market; larger quantities could be used as a bomb material.

The first nuclear-powered vessel, was a U.S. submarine launched in 1955, the USS *Nautilus*. Only three civil vessels (one U.S.-made, one German, and one Japanese) have ever been propelled by nuclear power; all proved too expensive to operate. About 160 nuclear-powered ships, mostly military, are presently at sea; at the peak of the Cold War, there were approximately 250.

#### ■ FURTHER READING:

##### BOOKS:

Glasstone, Samuel, and Alexander Sesonske. *Nuclear Reactor Engineering. Vol. I: Reactor Design Basics*. New York: Chapman & Hall, 1994.

Todreas, Neil E., and Mujid S. Kazimi. *Nuclear Systems I: Thermal Hydraulic Fundamentals*. New York: Hemisphere Publishing Corporation, 1990.

#### SEE ALSO

*Nuclear Detection Devices*  
*Nuclear Emergency Support Team, United States*  
*Nuclear Power Plants, Security*  
*Russian Nuclear Materials, Security Issues*

## Nuclear Regulatory Commission (NRC), United States

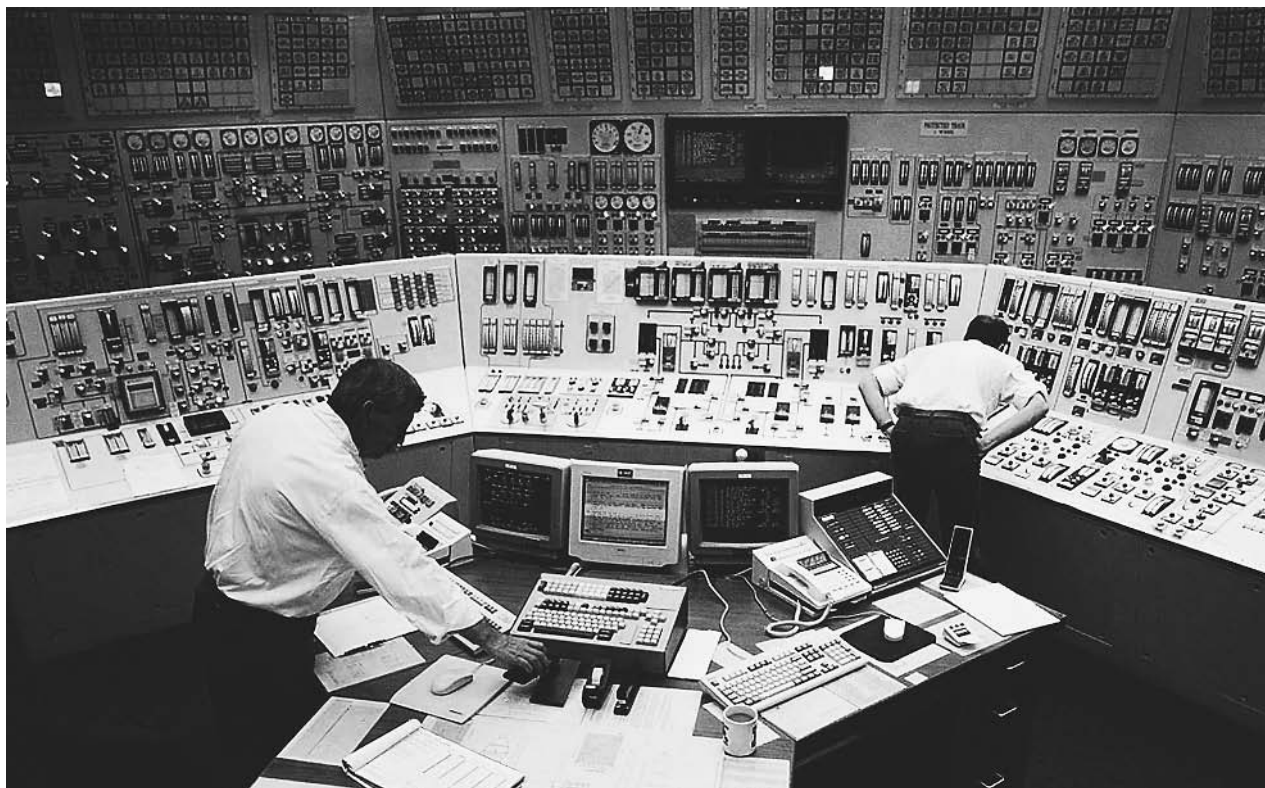
Established by the Energy Reorganization Act of 1974, the Nuclear Regulatory Commission (NRC) is an independent agency of the federal government tasked with regulating civilian use of nuclear materials. It deals with spent nuclear reactors, radioactive waste, and nuclear and source material, including thorium and isotopes of uranium. Among the important events of the NRC's early history was its handling of the Three Mile Island nuclear incident in 1979. Following the September 11, 2001, terrorist attacks, NRC officials were forced to contemplate the scenario of a similar terrorist attack upon a nuclear power plant.

### Organization and Responsibilities

The NRC is directed by a five-member commission, one of whose members is designated by the president of the United States as chairman and official spokesperson. The commission formulates policies and regulations regarding the safety of nuclear reactors and materials, issues orders to licensees, and adjudicates legal matters on nuclear power that are brought to its attention.

Answering to the commission is the executive director for operations (EDO), who carries out its policies and decisions, and oversees a number of offices. In addition to bureaus designated according to area of responsibility, the NRC has four regional offices, in the Atlanta, Philadelphia, Chicago, and Dallas areas. These oversee inspection, enforcement, and emergency response programs for licensees within their respective quadrants of the nation.

Among the other NRC offices, which collectively work to ensure the safe commercial use of nuclear power, are the offices of nuclear regulatory research, state and tribal programs, investigation, enforcement, and nuclear security and incident response. The last of these includes divisions for nuclear security, threat assessment, reactor



Workers man the control room of the Davis-Besse Nuclear Station in Oak Harbor, Ohio. The Nuclear Regulatory Commission, after an examination of the facility, concluded that no radiation was released after the plant took a direct blow from a tornado in 1998. AP/WIDE WORLD PHOTOS.

safeguards, materials safeguards, information security, and incident response.

**Overseeing plants, materials, and waste.** Two offices are together responsible for the actual oversight of nuclear materials and the plants that produce them. The Office of Nuclear Material Safety and Safeguards oversees nuclear waste and radioactive materials, while the Office of Nuclear Reactor Regulation is concerned with reactors.

Nuclear materials are divided into three types, all of which pose potential health and environmental hazards if not handled properly. Source material includes natural uranium and thorium, as well as depleted uranium. Byproduct material is nuclear material that has been made radioactive in a nuclear reactor, as well as tailings and waste produced by the extraction or concentration of uranium or thorium. A third variety of nuclear material poses an additional hazard, one of security. This category is known as special nuclear material, including uranium-233 and uranium-235, enriched uranium, and plutonium—any of which could be used in a nuclear device.

Regulated waste is also divided into three categories: low-level waste, including radioactively contaminated protective clothing, tools, and other materials; high-level waste, or used nuclear fuel; and uranium mill tailings, or the

residues remaining in natural ore after uranium and thorium have been extracted. As with the handling of nuclear materials, the Office of Nuclear Material Safety and Safeguards provides strict guidelines regarding the storage and disposal of these waste products.

Reactors regulated by the Office of Nuclear Reactor Regulation fall into two categories: power reactors, or commercial reactors used to generate electric power, and non-power reactors, or reactors used in research, testing, and training. Among the areas of responsibility for the office are reactor decommissioning, operator licensing, and new reactor licensing.

## History of the NRC

Prior to the advent of the NRC, the Atomic Energy Commission (AEC), established by Congress with the Atomic Energy Act of 1946, regulated nuclear energy. The Atomic Energy Act of 1954, which superseded its predecessor, legalized the development of commercial nuclear power for the first time in history. Among the provisions of the act was the assignment to the AEC of various functions relating to nuclear power production, including promotion of nuclear power and regulation of safety.

By the 1960s, the AEC had come under criticism for what many regarded as its failure to exercise sufficient

rigor in a number of areas, including reactor safety, environmental protection, and standards for radiation protection. In 1974, Congress abolished the AEC with the Energy Reorganization Act, which in turn replaced it with the Energy Research and Development Administration (established as the Department of Energy in 1977) and the NRC.

**Concerns over nuclear power.** As the NRC began operations on January 19, 1975, public sentiment against nuclear power was on the rise. The dissemination to mainstream society of environmentalist and anti-industrial ideas prevalent in the 1960s was a factor, as was lack of public understanding regarding the means by which nuclear power was generated and handled. Real bases for concerns existed, particularly with the dramatic increase in the size and number of nuclear plants that occurred during the late 1960s and early 1970s. Then, on March 28, 1979, an accident at the Three Mile Island plant outside Harrisburg, Pennsylvania caused half the reactor's core to melt.

In 1979, the modern system of around-the-clock news reporting via cable channels still lay many years in the future, yet for a few days in the spring of 1979, America followed the Three Mile Island catastrophe through regular news reports. No one died at Three Mile Island, and thanks in part to the NRC's efforts, the federal government dealt with the situation effectively. In the aftermath of Three Mile Island, the NRC placed a much greater emphasis on training of plant operators, studying plant histories for signs of vulnerability, and guarding against the failure of equipment.

During the 1970s, the rise of international terrorism, as well as the proliferation of nations hostile to the United States, spurred NRC leadership to take measures toward the protection of nuclear materials from theft or sabotage. Yet, in the aftermath of the September 2001, terrorist attacks, many critics maintained that power plants were vulnerable, and that the NRC was not taking appropriate measures to address the problem.

Given the destruction wreaked by the planes that flew into the World Trade Center and Pentagon, the September 11 attacks raised real fears concerning the vulnerability of nuclear plants. Questioned about the likelihood of damage from such an attack, an NRC spokesperson initially stated that these facilities could withstand an attack by a jet, but later admitted that "nuclear power plants were not designed to withstand such crashes."

#### ■ FURTHER READING :

##### BOOKS:

Walker, J. Samuel, and George T. Mazuzan. *Containing the Atom: Nuclear Regulation in a Changing Environment, 1963–1971*. Berkeley: University of California Press, 1992.

———. *Permissible Dose: A History of Radiation Protection in the Twentieth Century*. Berkeley: University of California Press, 2000.

##### PERIODICALS:

Hirsch, Daniel. "The NRC: What, Me Worry?" *Bulletin of the Atomic Scientists* 58, no. 1 (January/February 2002): 38–44.

Swanekamp, Robert. "Nuclear Renaissance Converges on Life Extension and Upgrades." *ENR* 247, no. 23 (December 3, 2001): PC54.

##### ELECTRONIC:

U.S. Nuclear Regulatory Commission. <<http://www.nrc.gov/>> (April 15, 2003).

##### SEE ALSO

*Chernobyl Nuclear Power Plant Accident, Detection and Monitoring*  
*DOE (United States Department of Energy)*  
*EPA (Environmental Protection Agency)*  
*International Atomic Energy Agency (IAEA)*  
*NNSA (United States National Nuclear Security Administration)*  
*Nuclear Power Plants, Security*  
*Nuclear Reactors*

## Nuclear Spectroscopy

■ K. LEE LERNER

Nuclear spectroscopy is a powerful tool in the arsenal of scientists and forensic investigators because it allows detailed study of the structure of matter based upon the reactions that take place in excited atomic nuclei. It is a widely used technique to determine the composition of substances because it is more sensitive than other spectroscopic methods and can detect the trace presence of elements in an unknown substance that may only be present on the order of parts per billion. Nuclear spectroscopic analysis techniques provided forensic investigators with evidence that linked several of what were eventually to be known as the Washington area "sniper shootings" in late 2002.

**Basic principles.** A number of methods can be used to excite atomic nuclei and then measure their decaying gamma ray emissions as the atoms return to normal energy levels (i.e., their ground state). The emissions are then analyzed and separated into an emission spectrum that is characteristic for each element. Excitation can be accomplished by colliding nuclei, heavy ion beams, and a number of other methods, but the fundamental purpose remains to measure the spectral properties of a sample as a tool to learn something about the quantum structure of the atoms in the sample.

Like other forms of spectroscopy, the fundamental measurements of nuclear spectroscopy involve recording the emission or absorption of photons by atoms. The specific emissions or absorptions reflect the energy levels, spin states, parity, and other properties of an atom's structure (e.g., quantized energy levels). A qualitative analysis identifies the components of a substance or mixture. Quantitative analysis, on the other hand, measures the amounts or proportions of those components. Because each element—and each nuclide (i.e., an atomic nucleus with a unique combination of protons and neutrons)—emits or absorbs only specific frequencies and wavelengths of electromagnetic radiation, nuclear spectroscopy is a qualitative test (i.e., a test designed to identify the components of a substance or mixture) to determine the presence of an element or isotope in an unknown sample.

In addition, the strength of emission and absorption for each element and nuclide can allow for a quantitative measurement of the amount or proportion of the element in an unknown. To perform quantitative tests, that is, to measure amounts of an element present, the measured spectrum needs to be narrowed down to analysis of photons with specific energies (i.e., electromagnetic radiation of a specific wavelength or frequency). Quantitative computation using Beer's Law is then applied to the measured intensities of photon emission or absorption. Many other spectroscopic methods use this technique (e.g., atomic absorption spectroscopy and UV-visible light spectroscopy) to determine the amount of a element present.

**Nuclear activation analysis.** One of most widely used methods of nuclear spectroscopy used to determine the elemental composition of substances is Nuclear activation analysis (NAA). In this type of analysis the goal is to determine the composition of an unknown substance by measuring the energies and intensities of the gamma rays emitted after excitation and the subsequent matching of those measurements to the emissions of gamma rays from standardized (known) samples. In this regard, neutron activation analysis is similar to other spectroscopic measurements that utilize other portions of the electromagnetic spectrum. Infrared photons, x-ray fluorescence, and spectral analysis of visible light are all used to identify elements and compounds. In each of these spectroscopic methods, a measurement of electromagnetic radiation is compared with some known quantum characteristic of an atomic nucleus, atom, or molecule. With NAA, of course, high-energy gamma-ray photons are measured.

Neutron activation analysis involves a comparison of measurements from an unknown sample with values obtained from tests with known samples. Depending on which elements are being tested for, the samples are irradiated with energetic neutrons. The process of radioactivity results in the emission of products of nuclear reactions (in this case, gamma rays) that are measurable

by instruments designed for that purpose. After a time (dependent on the duration of radiation) the gamma rays are counted by gamma ray sensitive spectrometers. Because the products of the nuclear reactions are characteristic of the elements present in the sample and a measure of the amounts present, neutron activation analysis is both a qualitative and quantitative tool. Although NAA usually involves the measurement of gamma rays emitted from the radioactive sample, more complex techniques also measure beta and positron emissions.

**Nuclear magnetic resonance.** Nuclear magnetic resonance (NMR) is another form of nuclear spectroscopy that is widely used in medicine and in forensic analysis. NMR is based on the fact that a proton in a magnetic field has two quantized spin states. The actual magnetic field experienced by most protons is, however, slightly different from the external applied field because neighboring atoms serve to alter it. As a result, a picture of complex structures of molecules and compounds can be obtained by measuring differences between the expected and measured photons absorbed. NMR spectroscopy is an important tool used to determine the structure of organic molecules.

When a group of nuclei are brought into resonance—that is, when they are absorbing and emitting photons of similar energy (electromagnetic radiation, e.g., radio waves, of similar wavelengths)—and then small changes are made in the photon energy, the resonance must change. How quickly and to what form the resonance changes allows for the non-destructive (because of the use of low-energy photons) determination of complex structures. This form of NMR is used by physicians as the physical and chemical basis of a powerful diagnostic technique termed Magnetic Resonance Imaging (MRI). MRI can also be used for non-invasive examinations for concealed substances or implanted objects.

#### ■ FURTHER READING:

##### BOOKS:

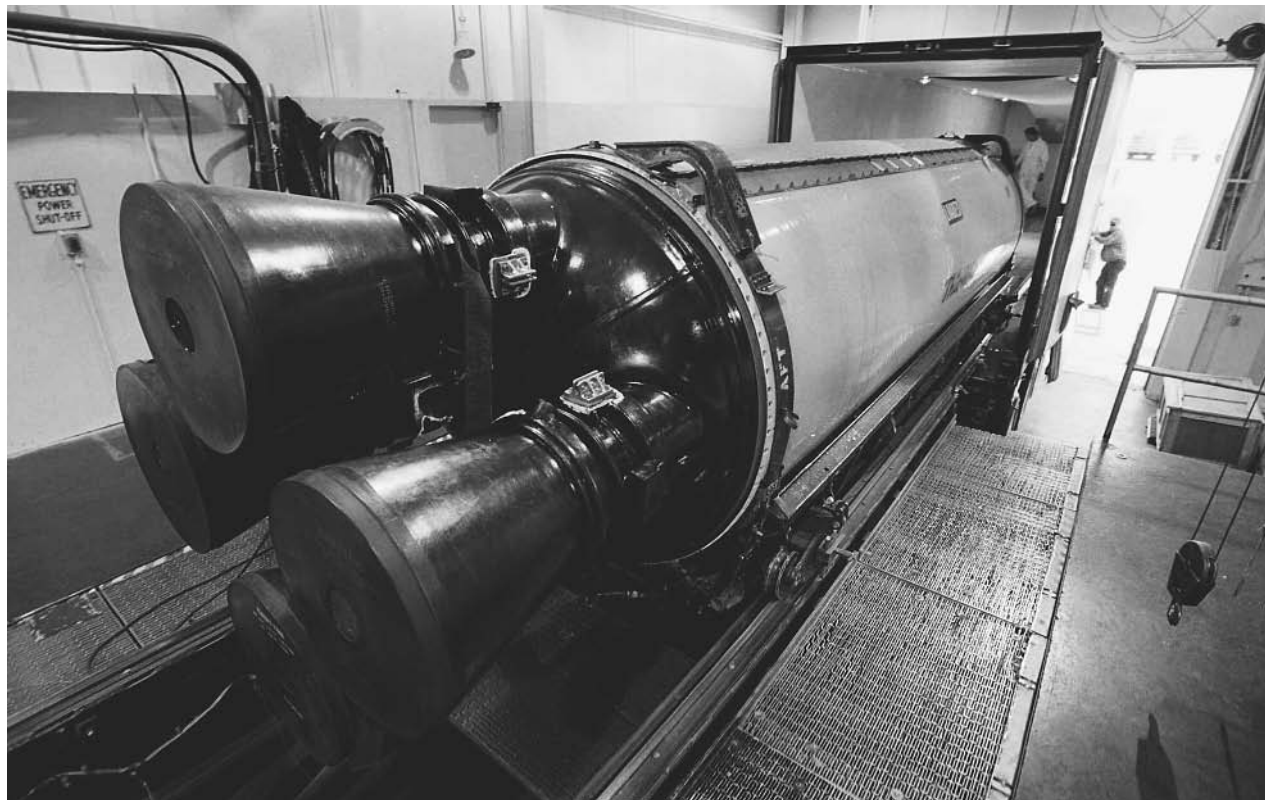
deGraaf, R. *In Vivo NMR Spectroscopy: Principles and Techniques*. New York: John Wiley & Sons, 1999.

##### SEE ALSO

*Electromagnetic Spectrum*  
*Scanning Technologies*

## Nuclear Waste.

SEE *Weapon-Grade Plutonium and Uranium, Tracking*.



A Minuteman III intercontinental ballistic missile engine is loaded into a truck in 2000 for transport to another building for refurbishment at Hill Air Force Base in Utah. AP/WIDE WORLD PHOTOS.

## Nuclear Weapons

■ LARRY GILMAN/K. LEE LERNER/  
DEAN ALLEN HAYCOCK

Nuclear weapons are explosive devices that utilize the processes of fission and fusion to release nuclear energy. An individual nuclear device may have an explosive force equivalent to millions of tons (megatons) of trinitrotoluene (TNT, the chemical explosive traditionally used for such comparisons), more than enough to completely destroy a large city. The destructive power of nuclear weapons derives from the core of the atom, the nucleus. One type of nuclear weapon, the fission bomb, uses the energy released when nuclei of heavy elements, such as plutonium, fission or split apart. A second even more powerful type of nuclear weapon, the fusion or hydrogen bomb, uses the energy released when nuclei of hydrogen are forced to fuse (join together).

Nuclear devices have been fashioned into weapons of many shapes with many purposes. Bombs can be dropped from airplanes; warheads can be delivered by missiles launched from land, air, or sea; artillery shells can be fired from cannons; mines can be placed on the land and in the sea. Some nuclear weapons are small enough

to destroy only a portion of a battlefield; others, as already mentioned, are large enough to destroy entire cities and more.

Unlike chemical explosives, nuclear weapons have had no peacetime uses, although in the 1950s the U.S. government briefly considered using them to blast artificial harbors in the Alaskan coastline. They are possessed by a number of nations, including the United States, France, Great Britain, China, India, Israel, Pakistan, and the Russian Federation along with several former Soviet Republics. Iran and North Korea, among other nations, are interested in building them. Since nuclear weapons were invented during World War II, they have been used only twice, both times against cities in Japan by the United States.

**Development of nuclear weapons.** German physicist Albert Einstein (1879–1955) did not know it at the time, but when he published his *Special Theory of Relativity* in 1905 he provided the world with the basic information needed to build nuclear weapons. Einstein said that the amount of matter of an object (i.e., its mass) is equivalent to a specific amount of energy. The exact amount of energy in an object equals its mass multiplied by the square of the speed of light. The speed of light is large—186,282 miles



per second (300,000 km/sec)—so even a small piece of matter contains a vast amount of energy. A baseball-size sample of uranium-235, for example, can explode with as much energy as 20,000 tons of TNT—and this involves the conversion of only a tiny fraction of the uranium's mass into energy. One pound of explosive material in a fission weapon is approximately 100,000 times as powerful as one pound of TNT.

As World War II approached, two German chemists, Fritz Strassmann (1902–1980) and Otto Hahn (1879–1968), pointed a stream of neutrons at a sample of uranium and succeeded in splitting the nuclei of some of its atoms. This splitting of nuclei is termed nuclear fission. The energy released through nuclear fission was the source of power for the first atomic bomb, which was built in the United States by a large team of scientists led by U.S. physicist J. Oppenheimer (1904–1967). This secret research and development program was termed the Manhattan Project.

The first atomic bomb was detonated in a test at Alamogordo, New Mexico, on July 16, 1945. Three weeks later, on August 6, a bomber named *Enola Gay* dropped a four-ton atomic bomb containing 12 lb (5.4 kg) of uranium-235 on the Japanese city of Hiroshima. Seventy thousand people died as a direct result of the blast. Within two months, nearly twice that many were dead from blast injuries and radiation. Three days later, on August 9, a bomb containing several pounds of plutonium was dropped on Nagasaki. Thirty thousand people died in the seconds following the explosion, and more later. The Japanese surrendered the next day, ending World War II.

These first nuclear weapons were atomic bombs or A-bombs. They depended on the energy produced by nuclear fission for their destructive power. However, scientists like U.S. physicist Edward Teller (1908–) knew even before the first atomic bomb exploded that the fission weapons could be used to create an even more powerful explosive, now called a thermonuclear device, hydrogen bomb, or H-bomb. This weapon gets its power from the energy released when atoms of the hydrogen isotopes deuterium or tritium are forced together, a process called nuclear fusion. Starting a nuclear fusion reaction is even more complicated than setting off a fission atomic bomb; it requires such heat to initiate it that a fission bomb is used as a detonator to explode the fusion bomb. The United States tested the first hydrogen bomb on November 1, 1952. It exploded with the force of 10.4 megatons (millions of tons of TNT equivalent). Three years later, the Soviet Union exploded a similar device.

For the next 40 years, the United States, with its allies, and the former Soviet Union, with its allies, raced to build more nuclear weapons, with each side producing tens of thousands. The end of the cold war and the breakup of the Soviet Union in the early 1990s led to the elimination of a significant number of nuclear weapons; however, the U.S. and Russia still possess many thousands of nuclear weapons.

**The physics and mechanics of nuclear weapons.** Conventional, chemical explosives get their power from the rapid rearrangement of chemical bonds, the links between atoms made by sharing electrons. In chemical explosives, atoms dissociate from other atoms and form new associations; this releases energy, but the atoms themselves do not change. Nuclear weapons are based on an entirely different principle. They derive their explosive power from changes in the structure of the atom itself, specifically, in the core of the atom, its nucleus.

Atomic bombs use the energy released when nuclei of heavy elements split apart or fission. Uranium and plutonium are the two elements that can be used as fuel for this type of weapon. When nuclei of these atoms are struck with rapidly moving neutrons, they are broken into two pieces nearly equal in size. They also release more neutrons, which split more nuclei. This is called a chain reaction. If enough atomic nuclei split they will release enough neutrons to ensure that all the nuclei of all the atoms in a sample will be split. Enormous amounts of energy are then released in a fraction of a second. This release of energy is the power behind the atomic bomb.

Uranium and plutonium are termed fissile materials because they can support a fission chain reaction if enough material is concentrated in one place. Too small a sample would not generate enough neutrons to keep the fission process going; for example, a one-pound (.45-kg) sample of uranium-235, a sample about the size of a ping-pong ball, is not large enough to support a chain reaction. The atomic bombs used in World War II proved that 12 or so pounds (about 5.5 kg) of fissile material, larger than a ping-pong ball but still small enough to fit into your hand, is enough to maintain a chain reaction. The smallest amount of material that can support a chain reaction is called the critical mass.

The instant enough bomb material is gathered together into a critical mass, a chain reaction begins. (At higher density, less mass is required.) This means that fissile material cannot be assembled in a critical mass until it is meant to explode. Therefore, the sample of uranium or plutonium in an atomic bomb is separated into several pieces, each of which is below critical mass. To set the bomb off, the separated pieces of bomb material are rammed together to create a critical mass. One design for creating a critical mass involves firing a subcritical "bullet" of fissile material into a subcritical "target" of fissile material. Together, the bullet and the target create a critical mass that starts a chain reaction leading to a nuclear explosion.

A different design was used to detonate the bomb dropped on Nagasaki. Plutonium was stored in one large but subcritical mass. It was compressed to a critical density by means of surrounding chemical explosives. When the chemical explosive detonated, the blast forced the bomb material into a density that reached criticality. In either type of design, once criticality is reached the explosion follows in a millionth of a second.

In order for nuclear fission to occur, a bomb must use heavy atoms for fuel. Heavy atoms have many nucleons—neutrons and protons—in their nuclei. When these heavy nuclei split apart they release energy (and neutrons, which may cause nearby heavy nuclei to split apart also). Another more powerful type of nuclear weapon uses forms of hydrogen as fuel. Hydrogen has few subatomic particles in its nuclei—usually only a proton, but the isotope deuterium has a proton plus a neutron, while the isotope tritium has a proton plus two neutrons. Instead of being split apart, these light atomic nuclei are forced together in high-speed collisions, a process called nuclear fusion. Energy is released when hydrogen nuclei fuse, forming helium. Fusion only occurs at temperatures of millions of degrees, such as exist in the hearts of stars. (The sun and other stars generate their energy primarily by fusing hydrogen into helium.) On Earth only an atomic bomb can raise kilograms of material to such a temperature, which is why atomic bombs are used as detonators for hydrogen fusion bombs.

Because hydrogen is lighter than uranium, more hydrogen atoms fit into a sample of the same weight. Thus, even though one fusion reaction releases less energy than one fission reaction, more hydrogen than uranium atoms can be packed into a nuclear weapon and many more fusion reactions can take place in the weapon than fission reactions can take place in a fission bomb. Fusion weapons, therefore, produce bigger explosions than fission weapons of the same physical bulk.

By 1954, a new feature had been added to the hydrogen bomb to create an even more dangerous weapon. Like earlier hydrogen bombs, this weapon was detonated with the explosion of an atomic or fission weapon. This raised temperatures enough to cause the hydrogen atoms in the bomb to fuse and explode like a regular hydrogen bomb. The designers also enclosed this new bomb in a shell of uranium-238. Neutrons released from the fusion of hydrogen caused the uranium-238 in the surrounding jacket to undergo fission, adding to the power of the blast. This new device was, in effect, a fission-fusion-fission bomb.

The power or “yield” of a nuclear weapon is expressed in terms of how much TNT would be required to equal the weapon’s blast. Units of kilotons (thousands of tons) and megatons (millions of tons) of TNT are used to describe nuclear blasts.

**Effects of nuclear weapons.** Nuclear weapons produce two important effects that are also produced by conventional, chemical explosives: they release heat and generate shock waves, or pressure fronts of compressed air that smash objects in their paths. The heat released in a nuclear explosion creates a sphere of burning, glowing gas that can range from hundreds of feet to miles in diameter, depending on the power of the bomb. This fireball emits a flash of heat that travels outward from the site of the explosion (ground zero), the area directly under the explosion. This heat can cause second degree burns to bare

human flesh miles away from the blast site if the bomb is large enough. (Although this heat can start fires, it seems that much of the fire damage in Hiroshima and Nagasaki following the nuclear explosions resulted from damaged electrical, fuel, gas, and other systems following physical damage caused by the shock or blast wave that accompanied the explosion.)

The shock wave produced when a nuclear weapon explodes creates a front of moving air more powerful than any produced by a natural storm. Destructive winds follow the front of displaced air, causing more damage to objects in their path. Many nuclear weapons are designed to be detonated high above their targets to take advantage of this shock effect. The more powerful the bomb, the higher in the sky it will be detonated. The fission bombs dropped on Japan (Hiroshima, 13.5 kilotons; Nagasaki, 22 kilotons) exploded between 1,500 and 2,000 feet (458–610 m) above their targets. A bomb with the power of 10 megatons is capable of destroying most houses within a distance of more than 10 miles from the blast site.

Unlike conventional explosives, nuclear devices can also release significant amounts of radioactivity and pulses of electromagnetic energy. Radioactivity is the release of fast particles and high-energy photons from unstable atomic nuclei. Besides the greater explosive power of nuclear weapons, radiation is the primary feature that most clearly distinguishes chemical from nuclear explosions. Radiation can kill outright at high doses and cause illnesses, including cancer, at lower doses. The initial burst of radiation during a nuclear explosion is made up of X rays, gamma rays, and neutrons. The energy of this radiation is so high that it can often penetrate buildings. Radioactive materials then contaminate the explosion site and often enter the atmosphere where they can travel thousands of miles before falling back to earth. This source of radiation is called radioactive fallout. Radioactive fallout can harm living things for years following a nuclear explosion. Fission bombs and fission-fusion-fission bombs produce more fallout than hydrogen bombs because the fusion of hydrogen atoms generates less radioactive by-products than does fission of uranium or plutonium.

Electromagnetic pulses (EMPs) are also produced by nuclear weapons that are exploded at high altitudes, and are caused by the interaction of radiation from the explosion with electrons in the atmosphere and with the Earth’s magnetic field. EMPs are essentially powerful radio waves that can destroy many electronic circuits.

The effects of fires and destruction following a large-scale nuclear war could even change the climate of the planet. In 1983 a group of scientists, including U.S. astronomer Carl Sagan (1934–1996), published the “nuclear winter” theory, which suggested that particles of smoke and dust produced by fires caused by many nuclear explosions would, for a time, block the Sun’s rays from reaching the surface of Earth. This, in turn, would reduce temperatures and change wind patterns and ocean currents. These climatic changes, according to the theory, could destroy crops and lead to the death by famine of many more

animals and humans than were killed outright by nuclear explosions. Some scientists have challenged these predictions, but others, including some United States government agencies, support them. On the other hand, there is no controversy about whether a large-scale nuclear war could kill hundreds of millions of people and imperil the future of modern civilization, even apart from nuclear winter effects.

**Modern nuclear weapons.** Today nuclear weapons are built in many sizes and shapes not available in the 1940s and 1950s, and are designed for use against many different types of military and civilian targets. Some weapons are less powerful than 1,000 tons of TNT, while others have the explosive force of millions of tons of TNT. Small nuclear shells can be fired from cannons. Nuclear warheads mounted on missiles can be launched from land-based silos, ships, submarines, trains, and large wheeled vehicles. Several warheads can be fitted into one missile and directed to different targets in the same geographic area upon reentry into the Earth's atmosphere. These multiple independently-targeted reentry vehicles (MIRVs) can release 10 or so individual nuclear warheads far above their targets, making enemy interception more difficult and increasing the deadliness of each individual missile.

In general, nuclear weapons with "low" yields (in the kiloton, rather than the megaton, range) are termed "tactical," and are designed to be used in battle situations against specific military targets, such as a concentration of enemy troops or tanks, a naval vessel, or the like. These weapons are termed tactical because the word tactics, in military jargon, refers to the relatively small-scale maneuvers undertaken to win particular battles. Larger nuclear weapons are classed as "strategic," because the word strategy, again in military jargon, refers to the large-scale maneuvers undertaken to win whole wars. Strategic nuclear weapons are targeted mostly at cities and at other nuclear weapons, and are generally designed to be dropped by bombers or launched on ballistic missiles; tactical nuclear weapons are delivered by smaller devices over shorter distances. However, one nation's "tactical" warhead may be another's "strategic" warhead: Russia, for example, maintains that U.S. tactical warheads in Western Europe are in fact strategic warheads, because they can strike targets inside Russia itself, while Russian "tactical" warheads in the same arena cannot strike the U.S. heartland.

In the summer of 2002, the George W. Bush administration sought and received permission from Congress to design a new class of nuclear weapons: "mini-nukes" are relatively low-yield tactical nuclear weapons for use against underground bunkers and other small battlefield targets. Also in 2002, the U.S. military—according to a secret Pentagon document leaked to the press—drew up an official set of contingency plans for attacking seven countries with nuclear weapons (China, Russia, Iraq, North Korea, Iran, Libya and Syria). Advocates of these new weapons point to the uniquely powerful, compact "punch" that can be delivered by a nuclear weapon; critics argue

that even a small nuclear weapon may cause many civilian casualties, and, more important, that actual use of a nuclear weapon of any size would break the taboo on such use that has held since the end of World War II, making the use of larger, more destructive nuclear weapons more likely in future conflicts. Some analysts stressed that the Pentagon's explicit willingness to use nuclear weapons in a "first-use" fashion, that is, in response to "unexpected military situations" not involving attack on U.S. forces by nuclear weapons, or to use them on targets (e.g., deep bunkers) resistant to conventional explosives signaled a major shift in United States nuclear use doctrine.

Even the ability of nuclear weapons to release radioactivity has been exploited to create different types of weapons. "Clean bombs" are weapons designed to produce as little radioactive fallout as possible. A hydrogen bomb without a uranium jacket would produce relatively little radioactive contamination, for example. A "dirty bomb" could just as easily be built, using materials that contribute to radioactive fallout. Such weapons could also be detonated near Earth's surface to increase the amount of material that could contribute to radioactive fallout. "Neutron" bombs have been designed to shower battle fields with deadly neutrons that can penetrate buildings and armored vehicles without destroying them. Any people exposed to the neutrons, however, would die. (Neutron bombs also destroy with blast effects, but their deadly radiation zones extend far beyond the site of their explosions).

The United States and Russia signed a Strategic Arms Reduction Treaty in 1993 to eliminate two thirds of their nuclear warheads in 10 years. By 1995, nearly 2,500 nuclear warheads had been removed from bombers and missiles in the two countries, according to U.S. government officials. ("Elimination," in this context, does not necessarily mean dismantlement; many of the weapons that have been "eliminated" by the treaty have been put in storage.) Although thousands of nuclear weapons still remain in the hands of many different governments, especially those of the U.S. and the Russian Federation, recent diplomatic trends have at least helped to lower the number of nuclear weapons in the world. This has caused many people to assume that the danger of nuclear weapons evaporated with the end of the Cold War.

However, the number of nations possessing nuclear weapons continues to increase, and the possibility of nuclear weapons being used against human beings for the first time since World War II may be larger than ever. In May 1995, more than 170 members of the United Nations agreed to permanently extend the Nuclear Non-Proliferation Treaty, first signed in 1960. Under the terms of the treaty, the five major countries with nuclear weapons—the United States, Britain, France, Russia, and China—agreed to commit themselves to eliminating their arsenals as an "ultimate" goal. The other 165 signatory nations agree not to acquire nuclear weapons. Israel, which is believed to possess nuclear weapons (but officially denies doing so), did not sign the treaty. Two other nuclear

powers also refused to renounce nuclear weapons: India and Pakistan, each of which probably possess several dozen nuclear weapons, have fought a number of border wars in recent decades, and in 2002 came close, as many observers thought, to fighting a nuclear war. As of 2003, North Korea had reactivated its nuclear-weapons-material production facilities and was engaged in a tense diplomatic standoff with the United States, which insisted that North Korea abandon its nuclear-weapons program.

## ■ FURTHER READING:

### BOOKS:

- Rhodes, Richard. *Dark Sun: The Making of the Hydrogen Bomb (Sloan Technology Series)*. New York: Simon & Schuster, 1995.
- Sagan, Scott D. and Kenneth N. Waltz. *The Spread of Nuclear Weapons: A Debate Renewed*, 2nd ed. W. W. Norton & Co., 2003.
- Walmer, Max. *An Illustrated Guide to Strategic Weapons*. New York: Prentice Hall Press, 1988.

### ELECTRONIC

- "U.S. Has Nuclear Hit List." BBC News. March 2, 2002. <<http://news.bbc.co.uk/2/hi/americas/1864173.stm>> (Feb. 26, 2003).

### SEE ALSO

- Arms Control, United States Bureau*  
*Iranian Nuclear Programs*  
*Manhattan Project*  
*North Korean Nuclear Weapons Programs*  
*Nuclear Detection Devices*  
*Russian Nuclear Materials, Security Issues*  
*World War II*

---

## Nuclear Winter

---

### ■ AGNES GALAMBOSI

Nuclear winter is a meteorological theory estimating the global climatic consequences of a nuclear war—or a natural disaster such as a major asteroid impact—that injects large amounts of dust or water vapor into the atmosphere. Nuclear winter models predict prolonged and worldwide cooling and darkening caused by the blockage of sunlight.

During the Cold War, concern about the use of nuclear weapons initially concentrated on initial blast damage and the dangers of radioactive fallout. Subsequently, researchers began to explore the possible environmental effects of nuclear war. The term nuclear winter was first defined and used by American astronomer Carl Sagan (1934–1996) and his group of colleagues in their 1983 article (later referred to as the TTAPS-article, from the initials of the authors' family names). This article was the

first one to take into consideration not only the direct damage, but also the indirect effects of a nuclear war.

During a nuclear war, the exploding nuclear warheads would create huge fires, resulting in smoke and soot from burning cities and forests being emitted into the troposphere in vast amounts. According to nuclear winter theory, this would block the Sun's incoming radiation from reaching the surface of Earth, causing cooling of the surface temperatures. The smoke and soot soon would rise to high altitude because of their high temperature and drift there for weeks without being washed out. Finally, the particles would settle in the Northern Hemisphere mid-latitudes as a black particle cloud belt, blocking sunshine for several weeks.

The ensuing darkness and cold, combined with nuclear fallout radiation, would kill most of Earth's vegetation and animal life, which would lead to starvation and diseases for the human population surviving the nuclear war itself. At the same time, because the smoke would absorb sunlight, the upper troposphere temperatures would rise and create a temperature inversion causing further retention of smog at the lower levels. Another predicted consequence is that nuclear explosions would produce nitrogen oxides that would damage the protective ozone layer in the stratosphere and allow more ultraviolet radiation to reach Earth's surface.

Although the basic findings of the original TTAPS-article have been confirmed by later reports and sophisticated computer modeling, some later studies report a lesser degree of cooling that would last for weeks instead of the initially estimated months. In the extreme, however, depending on the number of nuclear explosions, their spatial distribution, targets, and many other factors, a cloud of soot and dust could remain for many months, reducing sunlight almost entirely and decreasing average temperatures to well below freezing over a majority of the densely inhabited areas of the Northern Hemisphere.

The nuclear winter scenario remains scientifically controversial because the exact level of atmospheric damage, along with the extent and duration of subsequent processes cannot be agreed upon with full confidence. Opponents of the nuclear winter theory argue that there are many problems with the hypothesized scenarios either because of the model's incorrect assumptions (e.g., the results would be right only if exactly the assumed amount of dust would enter the atmosphere, or because the model assumes uniformly distributed, constantly injected particles). Other critics of the nuclear winter scenario point out that the models used often do not include processes and/or feedback mechanisms that may moderate or mitigate the initial effects of nuclear blasts on the atmosphere (e.g., the moderating effects of the oceans). In contrast to nuclear winter models, some climate models actually postulate a "nuclear summer," resulting from a worldwide warming caused by many small contributions to the greenhouse effect from carbon dioxide, water vapor, ozone, and various aerosols entering the troposphere and stratosphere.

What all scenarios and models forecast, however, is that a nuclear war would have a significant effect on the atmosphere and climate of Earth. This in turn would drastically and negatively affect many aspects of life such as food production and energy consumption.

#### ■ FURTHER READING :

##### BOOKS:

*International Seminar on Nuclear War and Planetary Emergencies, 20th Session: The Role of Science in the Third Millennium, Man-Made & Natural Disasters, Post-Berlin-Wall Problems-Nuclear Proliferation in the Multipolar World.* Singapore: World Scientific Publishing, 1997.

Weinberger, Casper. "The Potential Effects of Nuclear War on the Climate." *Nuclear Winter, Joint Hearing before the Committee on Science and Technology and the Committee on Interior and Insular Affairs, U.S. House of Representatives.* Washington, D.C.: Government Printing Office, 1985.

##### PERIODICALS:

Ehrlich, Paul, et al., "Long-Term Biological Consequences of Nuclear War." *Science* 222, 4630 (1983).

Turco, R. P., O. B. Toon, T. P. Ackerman, J. B. Pollack, and Carl Sagan. "Nuclear Winter: Global Consequences of Multiple Nuclear Explosions." *Science* 222, 4630 (1983).

White Paper. "Nuclear Winter: Scientists in the Political Arena." *Physics in Perspective* 3:1 (2001):76–105.

##### SEE ALSO

*Nuclear Detection Devices*  
*Nuclear Emergency Support Team, United States*  
*Radiation, Biological Damage*  
*Radiological Emergency Response Plan, United States*  
*Federal*

---

## Nucleic Acid Analyzer (HANAA)

---

#### ■ AGNIESZKA LICHANSKA

HANAA is an acronym for the hand-held advanced nucleic acid analyzer. It was developed by the Lawrence Livermore National Laboratory in 1999 based on a previous model of the nucleic acid analyzer ANAA produced in 1997. HANAA is a real time polymerase chain reaction (PCR) based system for detecting pathogens (disease-causing organisms). It is highly sensitive as it can detect 200 organisms per milliliter. Although a number of rapid real time PCR instruments were constructed, HANAA is the first hand-held device allowing easy testing of samples directly in the field, and was employed by the United Nations inspectors in Iraq during their 2003 searches for biological weapons.

## Technology behind HANAA

The instrument takes advantage of real time PCR technology that was developed in recent years. PCR amplification of DNA requires repetitive sample heating (to approximately 95°C (or 203°F) and cooling to a lower temperature specific for the sample (usually 50–72°C, or 122–161°F). Traditional instruments require two to three hours to complete a PCR run and additional time to run the products on a gel to detect positive samples. New real-time PCR instruments have heating and cooling systems allowing a reduction of the running time to less than 30 minutes. The same instruments also allow observation of product formation during the run. This is achieved by incorporation of fluorescent detection methods to visualize product formation.

The main part of the instrument is a sample module containing a miniaturized silicon thermal cycle of high heating and cooling efficiency. These small thermal units are a major breakthrough in technology as they can be efficiently supported by batteries. In comparison, most of the existing real-time systems are comparatively larger and heavier and cannot be operated in the field with ease, despite the similarly good technology for detection or time of analysis. HANAA also has an advantage over its predecessor ANAA, which was as big as a small suitcase. HANAA fits into a palm and weighs just under one kilogram (around two pounds). It can operate 1.4 to 5.5 hours depending on the battery used. A run on the instrument is approximately 7–20 minutes depending on the program used for detection.

The PCR process used by HANAA is based on using TaqMan-type probes, which rely on a short DNA oligonucleotide being labeled by two fluorescent molecules, a quencher and a reporter. When a probe anneals to DNA, there is no signal as the short distance between the quencher and the reporter results in the reporter's fluorescence being quenched. However, during amplification, the reporter molecule is released and an increase in fluorescence is observed.

HANAA has four chambers for analysis and can perform two independent identifications in each chamber, therefore it is able to test for up to eight pathogens at one time. Each of the sample units can be run independently, which makes the instrument highly flexible in use. The unit is operated by a keypad, with all the menu options and results displayed on a LCD (liquid crystal display) screen as text or bar charts. A positive sample is announced by an audible alarm.

The instrument and technology are still dependent on the quality of the sample and lack of any possible PCR inhibitors in the sample. However, sample preparation is relatively simple. A template for PCR is prepared by placing sample in a liquid buffer in a small (0.020 ml) test tube and reagents are added directly to the same tube.

Potential uses for HANAA are in the areas of pathogen detection, military or counter-terrorist applications by army

and police, identification of genetically modified organisms (Department of Agriculture), and diagnostic at the first point of contact, especially in a case of bioterrorist attack. The main advantage of the instrument is the ease of operation, coupled with the short training time (just a one-day session is required).

■ FURTHER READING:

ELECTRONIC:

Lawrence Livermore National Laboratories. "Chemical and

Biological Detection Technologies." <<http://www.llnl.gov/nai/rdiv/chbio.html>> (15 January 2003).

Ronald Koopman et al. HANAA: Putting DNA Identification in the Hands of First Responder. <[http://coffee.phys.unm.edu/BTR/2001%20Conference/pdf/Koopman\\_Ronald.pdf](http://coffee.phys.unm.edu/BTR/2001%20Conference/pdf/Koopman_Ronald.pdf)> (15 January 2003).

SEE ALSO

*Biological Weapons, Genetic Identification*  
*DNA Fingerprinting*  
*DNA Recognition Instruments*  
*DNA Sequences, Unique*  
*Polymerase Chain Reaction (PCR)*



## Oak Ridge National Laboratory (ORNL)

Oak Ridge National Laboratory (ORNL) is a United States National Laboratory managed for the U.S. Department of Energy (DOE) by UT-Battelle, LLC. In addition to basic scientific research, ORNL conducts research projects and isotope production designed to contribute to national security.

The 58-square-mile Oak Ridge facility was originally known as the Clinton Laboratories or Clinton Engineering Works, but in 1943 ORNL was tasked with the separation of plutonium for the Manhattan Project (the U.S program during World War II to develop an atomic bomb). During the war, the Oak Ridge site became one of three major laboratories developed for the Manhattan Project—the others were located at Hanford, Washington, and Los Alamos, New Mexico.

Bomb design work and testing was completed at Los Alamos under the leadership of the physicist J. Robert Oppenheimer, but the critical fuel production problems were solved, and actual fuel production work completed, at the Oak Ridge and Hanford sites. The Oak Ridge site was chosen, in part, because the Tennessee Valley Authority (TVA) was able to supply the large electrical requirements of isotope separation equipment. At the Oak Ridge site, the process of gaseous diffusion was used to extract the U-235 isotope from uranium ore. By early 1945, the Oak Ridge lab was capable of producing uranium-235 purified to weapons grade use.

The modern ORNL staff includes more than 1500 scientists and engineers and more than 200 support and administrative personnel. In addition, ORNL annually hosts approximately 3000 additional visiting scientists and engineers who collaborate on specific projects. To the extent that research complements DOE missions or enhances

national security issues, ORNL personnel are allowed to collaborate on research projects for non-DOE sponsors.

The Oak Ridge research program encompasses the Oak Ridge National Laboratory (ORNL), Oak Ridge Institute of Science and Education (ORISE), and Thomas Jefferson National Accelerator Facility (Jefferson Lab). Oversight of ORNL is also coordinated by Oak Ridge Associated Universities, a not-for-profit consortium of 86 colleges and universities.

Environmental remediation and nuclear waste disposal issues are a part of the majority of ORNL programs. In addition to providing global assistance and expertise in remediation matters, ORNL scientists and engineers also use those skills and technologies in clean-up operations at the Oak Ridge Reservation; past research efforts have left portions of the site contaminated with nuclear and chemical waste. The Environmental Protection Agency (EPA) lists Oak Ridge among the nation's clean-up priorities.

The Y-12 National Security Complex houses many of the most secret national security projects, including research on nuclear weapon components and nuclear propulsion systems for the U.S. Navy. Among other ORNL advances is the refinement of a Chemical Biological Mass Spectrometer (CBMS) used in the enhanced detection of chemical and biological agents.

ORNL also produced the Raman Tunable Integrated Sensor (RAMiTS) used by inspectors and first responders to detect chemical agents (including explosive agents). The portable unit weighs only 40 pounds and includes a 12-foot fiber-optic sensing probe that allows inspectors to examine suspected agents from a safer distance.

In conjunction with other national laboratories and DOE Joint Genome Institute (JGI), ORNL researchers are advancing means of rapid DNA sequencing that can be used to identify and characterize specific microbial pathogens.

Other ORNL bioscience projects include research on artificial neural network engineering.



Researchers at the Oak Ridge National Laboratory in Oak Ridge, Tennessee, test a portable chemical and biological agent monitor developed for the army and marines in 2001. AP/WIDE WORLD PHOTOS.

ORNL scientists also form a key component of the Stockpile Stewardship and Management Program (SSMP), operated primarily by the Lawrence Livermore National Laboratory (LLNL). The SSMP program is designed to ensure that U.S. nuclear weapons remain reliable without detonation testing.

■ FURTHER READING :

ELECTRONIC:

Environmental Measurements Laboratory. National Security. <<http://www.eml.doe.gov/>> (March 16, 2003).

United States Department of Energy, Office of Science. National Laboratories and User Facilities. <[http://www.sc.doe.gov/Sub/Organization/Map/national\\_labs\\_and\\_userfacilities.htm](http://www.sc.doe.gov/Sub/Organization/Map/national_labs_and_userfacilities.htm)> (March 23, 2003).

United States Department of Homeland Security. Research & Technology. <<http://www.dhs.gov/dhspublic/display?theme=27&content=374>> (March 23, 2003).

SEE ALSO

*Argonne National Laboratory*

*Brookhaven National Laboratory  
DOE (United States Department of Energy)  
Environmental Measurements Laboratory  
Lawrence Livermore National Laboratory (LLNL)  
Los Alamos National Laboratory  
NNSA (United States National Nuclear Security Administration)  
Pacific Northwest National Laboratory  
Plum Island Animal Disease Center  
Sandia National Laboratories*

Official Secrets Act,  
United Kingdom

■ ADRIENNE WILMOTH LERNER

The Official Secrets Act of the United Kingdom prohibits the transfer of information deemed sensitive to national security interests. The first Official Secrets Act was passed





Former MI5 British secret agent David Shayler leaves London's Charing Cross police station after he was released on bail for charges of breaking the Official Secrets Act in 2000. AP/WIDE WORLD PHOTOS.

in 1889, and criminalized the sharing, disclosure, or publication of government information by employees and former employees of the intelligence and security forces. The act also covered the disclosure of information by journalists. The Intelligence Bureau, under the recommendation of the Committee for Imperial Defense, lobbied Parliament for the legislation. The act also codified the gathering of evidence to try an individual on the crime of treason based on espionage or the purveying of sensitive information. Parliament hurried the bill to passage, but some dissenters noted failings in the act, especially that the act did not grant explicit powers to search someone on suspicion of illegal activity and did not address new advances in technology, such as photography.

As tensions heightened in Europe in the years leading up to World War I, Parliament sought to broaden the Official Secrets Act. The newer act addressed some of the concerns raised in 1889 upon passage of the original legislation. The Official Secrets Act of 1911 included provisions criminalizing the sketching or photographing of restricted places, especially military installations.

While stipulating expanded criteria for illegal information, the 1911 act contained a few sweeping provisions that remained controversial for nearly 80 years. The Official Secrets Act of 1911 broadened the original act to give the government full discretion over what information would be considered illegal to disclose, and placed lifetime orders of silence on civil servants and security personnel regarding their actions and any confidential knowledge gained during their tenure of service.

The government did set forth some guidelines over the classes of information protected by the Official Secrets Act. Information provided by agents of foreign governments and organizations, security and intelligence forces, intercepted communications, and information related to crime and law enforcement was covered by the act. Opponents of the act cited the broadness of these categories, alleging that any government information or news could be construed to fit the designated categories.

Perhaps the largest controversy surrounding the act was that it gave scant consideration to tests for harm. It stipulated that no motive or proof of intent to cause harm

is necessary to prosecute, but that both can be inferred from a defendant's conduct, character, or associations. The law furthermore did not permit a defendant to claim that disclosure of information was in the public interest or that such information was already in the public domain. While criticism of the law subsided during wartime, it began to draw sharp criticism in the 1960s and 1970s from journalists who claimed the act allowed the government to cull the press of embarrassing information and prosecute journalists who used government employees as sources. Other opponents claimed it permitted government abuses in the intelligence and security forces to go unchecked, and failed to provide information to the public regarding security and terrorist threats.

In 1989, Parliament revisited the Official Secrets Act and replaced the long controversial Section 2 of the 1911 draft. The definition of secrets and information covered by the act was tightened to include only information deemed vital to national security and intelligence interests. Civil servants and military personnel wishing to report fraud and abuses now appeal to intra-government review boards, but are still prohibited from public disclosure of confidential government information, even if gained second-hand. Despite these revisions, the act remains contentious in Britain, especially among journalists who view the 1989 amendment as a negligible victory for freedom of information in the press.

#### ■ FURTHER READING :

##### ELECTRONIC:

Parliament of the United Kingdom. Select Committee on Public Administration, Third Report, 1998. <<http://www.parliament.the-stationery-office.co.uk/pa/cm199798/cmselect/cmpublicadm/398-vol1/39812.htm>> (January 2, 2003).

##### SEE ALSO

*United Kingdom, Intelligence and Security*

## One-Time Pad.

SEE *Cipher Pad*.

## OPEC (Organization of Petroleum Exporting Countries)

■ JOSEPH PATTERSON HYDER

The Organization of Petroleum Exporting Countries (OPEC) is a coalition of eleven nations that controls over fifty

percent of the world's oil and natural gas exports. OPEC members are Algeria, Indonesia, Iran, Iraq, Kuwait, Libya, Nigeria, Qatar, Saudi Arabia, United Arab Emirates, and Venezuela. OPEC strives to protect the economic interests of participating countries while maintaining a stable petroleum market by establishing production quotas for its member states.

Large Western oil companies controlled and profited from oil production in the Middle East and Africa in the first half of the twentieth century. The oil companies angered the leaders of these oil-rich countries by retaining 65 percent of the profits. OPEC was established in 1960 in order for the oil producing countries to maintain a larger percentage of oil-derived profits.

Although OPEC represented its members in negotiations with the large oil companies, the organization exercised little control over the world oil market until 1973. With inflation spiraling around the world and with increasing oil demands in the United States and Europe, OPEC realized that the stage was set for a major power grab.

Inflation led the Richard M. Nixon administration to place price controls on oil products in March 1973, resulting in increased demand. Faced with oil shortages because of increased demand, Nixon tapped U.S. oil reserves. By autumn 1973, the U.S. had nearly drained its reserves. The United States had become more dependent on oil imports than ever before.

The Yom Kippur War began in October 1973, with the United States and Western Europe supporting Israel over Egyptian and Syrian forces. OPEC, comprised primarily of Middle Eastern countries sympathetic to Egypt and Syria, made a move to seize increased control of the world oil market. OPEC imposed an oil embargo against the United States and increased oil prices in Europe. The price of crude oil doubled in a matter of days, from three U.S. dollars per barrel to over five dollars per barrel. In January 1974, prices reached 11.75 dollars per barrel.

The oil embargo of 1973–1974 inconvenienced frustrated Americans, who had to modify their lifestyles to accommodate the steep increase in oil prices. The White House encouraged Americans to conserve energy by driving less, carpooling, and turning down thermostats. The Nixon administration responded by extending Daylight Savings Time in the United States, encouraging companies to trim work hours, and pushing Congress to approve construction of the Alaskan Pipeline.

The energy crisis that resulted from the OPEC embargo fueled a worldwide recession. The Dow-Jones lost 45 percent over the next two years. Oil shortages led to long lines at gasoline pumps. When OPEC finally lifted the oil embargo against the U.S. in March 1974, it had established itself as one of the most powerful economic forces in the world.

OPEC's strategy backfired, however, when public and political opinion in the United States and Europe was inflamed. The United States increased its oil production with the completion of the Alaskan Pipeline in 1977. Large

American and European oil companies also sought to regain some of their lost influence by increasing oil exploration in non-OPEC countries and offshore. As a result, much of the power that OPEC had wielded over world energy markets was eroding.

For the first several years of the 2000s, OPEC sought a stable oil market by maintaining an average price of \$22 to \$28 per barrel of crude oil; exerting price controls had become more difficult and less profitable for members. An example of OPEC's increasing ineffectiveness occurred in 2001, when crude oil prices fell by one-third. During the same year, OPEC cut its oil production by over twenty percent.

OPEC has experienced periods of waning effectiveness in the past, but these periods were usually the result of internal disagreements. OPEC's more recent problems stem from the rise of large, non-OPEC oil producing states, such as Russia, Norway, Mexico, Oman, and Angola. In order for OPEC to remain a viable power, it needs the cooperation of these states. Russia, Norway, and Mexico have tended to follow OPEC's lead, but continued support from these states is questionable. Russia has already indicated that it will proceed independently for the foreseeable future.

Many OPEC members have expressed an unwillingness to limit their oil production and profits if non-OPEC countries continue pumping at full capacity and flooding the market with cheap oil. If OPEC cannot hold sway over these emerging oil-producing states, then the primary reason for the existence of OPEC may eventually be in question.

## ■ FURTHER READING:

### ELECTRONIC:

Organization of Petroleum Exporting Countries (OPEC). <<http://www.opec.org>> (May 2003).

### SEE ALSO

*Indonesia, Intelligence and Security*  
*Iran, Intelligence and Security*  
*Iraq, Intelligence and Security Agencies*  
*Kuwait Oil Fires, Persian Gulf War*  
*Libya, Intelligence and Security*  
*Nigeria, Intelligence and Security*  
*Saudi Arabia, Intelligence and Security*

Operation Liberty Shield, a specific set of measures designed to deter attack and protect Americans during periods of heightened risk of terrorism. The operation included a comprehensive and coordinated response among federal, state, and local authorities to an elevated threat level. Liberty Shield was designed to move the nation to a higher terror alert level in anticipation of the war against Iraq, imminent at that time.

Ridge announced that intelligence and law enforcement estimates indicated that terrorist groups and disgruntled individuals would "probably use military action in Iraq as pretext to attack." In raising the terror alert level to "high" (condition color orange), government officials automatically activated plans to disperse critical command and control elements of the government's emergency response forces and to restrict access to command operations. Operation Liberty Shield was specifically designed to augment these measures by staffing all response and recovery teams and to raise public awareness of both increased danger levels and specific protective measures.

As a component of Operation Liberty Shield, individuals seeking asylum for political purposes would be detained until their identity could be properly verified and their reasons for seeking asylum confirmed as legitimate. While all individuals seeking asylum would be temporarily detained, individuals from countries with known terrorist sympathies would receive extra screening and investigation.

Specific Liberty Shield measures included extended deployment of National Guard units and the positioning of those units alongside local law enforcement personnel to guard potential targets. Facilities designated as critical to the national infrastructure such as selected bridges, national landmarks, and medical and research facilities were put on special alert and in many cases, additional protective forces were deployed to those sites.

Liberty Shield operational plans called for heightened security at the nation's borders and additional Coast Guard patrols. Increased inspections were ordered at border crossings, and the Coast Guard stepped up its escorts of ships into harbor. Special security measures and enhanced screening was mandated for transportation facilities, including airport and railroad terminals. Railroads and trucking industries were ordered to increase inspections and protection of cargo.

Flight restrictions or limitations to operations were instituted over many United States cities. Flight restrictions were extended over some petroleum and all nuclear facilities. Additional guards were assigned to petroleum storage facilities, nuclear reactors, and nuclear waste sites.

As a part of Operation Liberty Shield, the FBI and Homeland Security personnel increased monitoring of individuals suspected of contributing to terrorist organizations and organizations suspected of funneling funds to terrorist organizations. Special units of agents and engineers were detailed to monitor Internet support facilities

---

## Operation Liberty Shield

---

On March 18, 2003, United States Secretary of Homeland Security Tom Ridge announced the implementation of

and to respond to possible cyberterrorism. Treasury agents instituted special computer-based checks to monitor and protect the nation's financial transfer systems.

To deter bioterrorism, state and local health departments were asked to be especially alert to and report unusual diseases, suspect symptoms, or suspicious disease patterns. Increased security measures were implemented in the nation's food supply network. Department of Agriculture officials ordered special inspections at feedlots, stockyards, and food distribution sites.

Ridge encouraged Americans to "be informed, stay alert, and report unusual activity." Additional details of emergency preparedness operations were posted at [www.ready.gov](http://www.ready.gov), a website maintained by the Department of Homeland Security. Ridge stated that during Liberty Shield operations, government officials would place special emphasis on public communications.

#### ■ FURTHER READING :

##### ELECTRONIC:

Department of Homeland Security. "Ready.gov." March 18, 2002. <<http://www.ready.gov/>> (March 18, 2003).

##### SEE ALSO

*Terror Alert System, United States*

## Operation Magic

■ ADRIENNE WILMOTH LERNER

Operation Magic was the cryptonym given to United States efforts to break Japanese military and diplomatic codes during World War II. The United States Army Signals Intelligence Section (SIS) and the Navy Communication Special Unit worked in tandem to monitor, intercept, decode, and translate Japanese messages. Intelligence information gathered from the messages was sent to military command at the Office of Strategic Services (OSS). The ability to decipher and read Japanese communications was one of the key components of the Allied victory in the Pacific.

Even before the outbreak of World War II in Europe in 1939, the United States began its efforts to decode Japanese diplomatic and military communications. In 1923, a United States Navy intelligence officer obtained a contraband copy of the World War I era Japanese Imperial Navy Secret Operating Code. Photographs of the codebook were passed on to the cryptologists at the Research Desk, where code was placed in red folders after the additive code keys were fully discovered. The simple additive code became known as "Red," after the folders in which it was stored.

For high-level communications, the Japanese replaced Red with Blue, a more sophisticated code in 1930. However, the new code too closely resembled its predecessor, allowing United States cryptologists to fully break the new cipher in less than two years. At the outbreak of World War II, the Japanese were still using both Red and Blue for various communications. U.S. military intelligence established listening stations throughout the Pacific to monitor ship-to-ship, command-to-fleet, and land-based communications.

After war broke out in Europe, the Japanese received encryption and security help from Nazi Germany. The Germans had discovered that U.S. intelligence was monitoring and decoding Japanese communications as early as 1935, but they did not immediately inform the Japanese. Later, Germany sent a copy of their infamous Enigma encryption machine, with a few modifications, to help secure Japanese communications. As a result, U.S. intelligence could no longer read Japanese intercepts. The painstaking work of U.S. cryptologists began anew.

U.S. cryptanalysts named the new code Purple. Applied to several variations of the initial Enigma code, Purple provided the most significant challenge to both United States and British intelligence during the war.

With the aid of information from Polish and Swedish cryptologists, the British military intelligence cryptanalysis unit at Bletchley Park first broke the German Enigma code. They then developed sophisticated decoding bombs and the first programmable computer to facilitate the deciphering of the complex Enigma code. By 1943, British intelligence was able to utilize almost real-time intelligence information received from translated Enigma intercepts.

In the United States, cryptologists struggled to break the Purple by hand. However, the structure of Japanese messages, always beginning with the same introductory phrase, aided code breakers in determining the sequencing of the multi-rotored Japanese cipher machine. United States code breakers had made significant progress on the Purple code by 1941, gaining the ability to read several lines of intercepts. The process remained slow, and the information gained from Purple was usually outdated by the time it was translated.

Aware of British successes against the German Enigma machine, United States military intelligence asked their ally to share code-breaking information. The British sent top Bletchley Park cryptographers and engineers to the United States to help train code breakers and build decoding bombs. However, they closely guarded, and did not share, the secret of Enigma code breaking efforts (code named Operation Ultra) that involved Colossus, the Bletchley Park decoding computer.

With the aid of the British, United States intelligence made significant progress against Purple in a short time. A replica of the Japanese Purple machine, built in 1939 by

American cryptologist William Friedman, was used to adapt a German Enigma bombe to decode Japanese Purple. Although the settings for each message had to be determined by hand, United States intelligence gained the ability to read Japanese code with greater ease, in a more timely manner, by 1942, six months after the Japanese bombing of Pearl Harbor and the entry of the United States into World War II.

Utilizing their extensive network of listening stations in the Pacific, United States intelligence intercepted and decoded several other types of messages. Diplomatic Purple messages, paired with JN-25 intercepts, another broken Japanese Navy code, gave U.S. military command vital information about Japanese defenses at Midway. Operation Magic intercepts provided useful information during the ensuing Battle of Midway, turning the tide of the war in the Pacific in favor of the allied forces. A year later, Purple intercepts gave the U.S. information about a diplomatic flight on which Japanese General Yamamoto, the mastermind behind the Pearl Harbor attack, was traveling. U.S. planes shot down the Japanese aircraft.

Operation Magic provided critical intelligence information in both the Pacific and European theaters of war. Diplomatic messages between Berlin and Tokyo, encoded with Enigma and Purple, yielded British and United States intelligence information regarding German defenses in France. The information helped commanders plan the D-Day invasion of Normandy in June 1944.

The Japanese government remained unaware that the United States broke the Purple code. Japanese Imperial forces continued to use codes broken by Operation Magic throughout the war and in the weeks following the Japanese surrender in 1945.

#### ■ FURTHER READING:

##### BOOKS:

- Boyd, Carl. *Hitler's Japanese Confidant: General Oshima Hiroshi and MAGIC Intelligence, 1941–1945*. Lawrence, KS: University Press of Kansas, 1993.
- Budiansky, Stephen. *Battle of Wits: The Complete Story of Codebreaking in World War II*. New York: Touchstone Books, 2002.
- Clark, Ronald William. *The Man Who Broke Purple: The Life of Colonel William F. Friedman, Who Deciphered the Japanese Code in World War II*. Boston: Little Brown, 1977.
- Matthews, Tony. *Shadows Dancing: Japanese Espionage Against the West*. New York: St. Martin's Press, 1993.

##### SEE ALSO

*Bletchley Park*  
*Bombe*  
*Purple machine*  
*Red code*  
*Ultra, Operation*

*World War II*  
*World War II, United States Breaking of Japanese Naval Codes*

## Operation Mongoose

■ ADRIENNE WILMOTH LERNER

In November 1961, following the disastrous Bay of Pigs invasion, President John F. Kennedy and his advisors launched Operation Mongoose, a covert operation intended to disrupt Cuban government and economic infrastructure. The ultimate goal of the operation was to thoroughly undermine, or even assassinate if necessary, Cuban revolutionary leader Fidel Castro. President Kennedy named his brother, United States Attorney General Robert Kennedy, to oversee Operation Mongoose. Robert Kennedy conducted Operation Mongoose in cooperation with President Kennedy's Foreign Intelligence Advisory Board, a group of civilian experts on foreign relations.

Before Kennedy's election, the CIA clandestinely explored the notion of assassinating Castro. Castro's communist policy and close ties with the Soviet Union unnerved administration officials. The physical proximity of Cuba to the United States added Cold War security risks. Based upon interviews and declassified materials, historians assert that in 1960 several senior CIA officials allegedly began working with members of the mafia. The mafia would give the CIA plausible deniability if the assassination plot were uncovered. The mafia had operatives in Cuba, and a motive for assassinating Castro, who had disrupted casinos, travel, and mafia business interests in Havana.

Although official confirmations and a great deal of evidence remains unavailable to the public, espionage historians assert that these talks reached a loggerhead and eventually dissipated just as the Kennedy Administration assumed control of the White House. One of the first priorities of the new administration was to address the situation of Cuba. To this end, Operation Mongoose was established. Mongoose was, in essence, a continuation of a secret operation against the Cuban regime that began during the Eisenhower Administration. Psychological operations (PsyOps) such as propaganda and staged incidents were part of the plan, but Mongoose also contained provisions for far more ambitious physical threats to Castro and his allies.

In 2001, 400 pages of documents relating to Operation Mongoose were declassified. These declassified documents show that Operation Mongoose had several primary objectives. The Kennedy Administration sought to disable or destroy power plants in Cuba, lay mines to

disrupt Cuban shipping, and undermine or destroy Castro's leadership. To achieve these goals, the Operation Mongoose creators proposed placing American intelligence operatives in Cuba.

The second objective of Operation Mongoose was to assassinate Castro. Operation Mongoose explored several possible means by which to carry out the assassination. The Kennedy administration considered poisoning cigars with *botulism* toxin and presenting them to Castro as a gift, poisoning a drink for Castro, and even rigging explosives to seashells on the sea floor to tempt the avid diver.

The final component of Mongoose was psychological warfare. Air Force Brigadier General Edward Lansdale commanded the PsyOps portion of Operation Mongoose. Lansdale created an anti-Castro radio broadcast that covertly aired in Cuba. Leaflets were distributed that depicted Castro as getting fat and wealthy at the expense of citizens. Operatives circulated stories about heroic freedom fighters.

Yet, the main thrust of Lansdale's plans was a series of large scale "dirty tricks" meant to evoke a call to arms against Cuba in the international community. One plan called for a space launch at Cape Canaveral to be sabotaged and blamed on Cuban agents. Operation Bingo called for a staged attack on the U.S. Navy Base at Guantanamo Bay in hopes of creating a mandate for the U.S. military to overthrow Castro.

When the Church Committee investigated the actions of the national intelligence agencies in the wake of the Watergate scandal in 1974, notes on Operation Mongoose surfaced for the first time. The committee commented not only on the assassination plots, but also noted the "dirty tricks" proposed by Lansdale. Little else was revealed about the operation for three more decades.

Ultimately, Operation Mongoose existed on paper more than in practice. While some elements of the initiative were attempted, such as elements of propaganda dissemination, the operation was abandoned by Kennedy's successor, President Johnson.

## ■ FURTHER READING :

### BOOKS:

Chang, Laurence, ed. *Cuban Missile Crisis, 1962: A National Security Archive Documents Reader*. Washington, D.C.: United States Government Press, 1998.

Fursenko, Alexandr and Timothy J. Naftali. *One Hell of a Gamble: Khrushchev, Castro, and Kennedy, 1958–1964*. New York: W.W. Norton and Company, 1998.

### SEE ALSO

*Church Committee*  
*Cuban Missile Crisis*

*Kennedy Administration (1961–1963), United States National Security Policy*

## Operation Shamrock

■ ADRIENNE WILMOTH LERNER

Operation Shamrock was a covert, domestic intelligence gathering operation that monitored telegraph communications. Shamrock began as a military intelligence program during World War II, but continued until the 1970s. The operation sparked controversy when details of Shamrock were leaked to the public after a government investigation in 1975. The government investigative committee claimed that Shamrock intended to monitor only messages that posed a threat to national security, but that it had free access to all wire traffic.

At its outset, Shamrock was a World War II military intelligence program. In the months before war broke out in Europe in 1939, the Army Signal Security Agency asked the three largest wire service companies, ITT World Communications, Western Union International, and RCA Global, for permission to tap their international cables to eavesdrop on foreign coded transmissions. The companies agreed, and Army Intelligence intercepted coded messages. Later, intelligence agents began to intercept all civilian and military wire traffic, both ciphered and plain-text.

Telegraph messages between the frontline and the home front were monitored and censored for sensitive content, such as troop locations and strategic battle plans. Military intelligence agents also sought to root out espionage communications and kept intercepts between political groups and other organizations with Axis sympathies. Thus, Shamrock was initially a wartime censorship program to cull sensitive information from the public domain in the interest of national security.

Shamrock continued, however, for nearly three decades after the end of World War II. At the war's end, Army Intelligence appealed to the major communications companies to continue their monitoring of international wire traffic. Their request was granted. When President Harry S. Truman created the National Security Agency (NSA) in 1952, the agency immediately took control of the ongoing telegraph communications monitoring. The program then acquired the code name Operation Shamrock. NSA authorities continued to monitor incoming and outgoing wire traffic from the monitoring station in New York. However, the transport of voluminous telegraph recording tape became difficult to transport. Technological advancements permitted the recording of the data on magnetic tapes, and to centralize the operation, the NSA created a New York office devoted to Shamrock. The office continued to operate until the mid 1970s, but the nature of

monitoring and recording information changed significantly since the program's inception.

After World War II, the focus of Shamrock shifted to follow Cold War policies. Shamrock sought to identify and monitor Soviet sympathizers, radical political organizations, international espionage agencies, and other perceived security threats. When the Vietnam conflict was at its height, Shamrock operatives kept lists of anti-war organizations and monitored communications of some individuals who fled the draft. These lists were code named Minaret, and by 1974 contained information on nearly 70,000 American citizens.

In 1975, the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, otherwise known as the Church Committee after its chairman, Senator Frank Church, conducted a comprehensive investigation of the U.S. intelligence agencies after the Watergate scandal. The Church Committee report concluded that Army intelligence and the NSA did have free access to wire traffic, and did compile information on private citizens. The committee further concluded that Shamrock did not continue past 1974, and that no further action or investigation of the matter was necessary.

#### ■ FURTHER READING:

##### ELECTRONIC:

United States National Security Agency. <<http://www.nsa.gov>>(03 January 2003).

##### SEE ALSO

*Church Committee*

## Operation Z.

SEE *Pearl Harbor, Japanese attack on.*

## Orange Volunteers (OV)

Orange Volunteers (OV) is a terrorist group that appeared in the late 1990s and is comprised largely of disgruntled loyalist hardliners who split from groups observing the cease-fire between Ireland and Northern Ireland. OV seeks to prevent a political settlement with Irish nationalists by attacking Catholic civilian interests in Northern Ireland. The group has been linked to pipe-bomb attacks and sporadic assaults on Catholics. Following a successful

security crackdown at the end of 1999, the OV declared a cease-fire in September 2000.

Operating principally in Northern Ireland, OV may have up to 20 dedicated members, some of whom are experienced in terrorist tactics and bombmaking.

#### ■ FURTHER READING:

##### ELECTRONIC:

CDI (Center for Defense Information), Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <<http://www.cdi.org/terrorism/terrorist.cfm>> (April 17, 2003).

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001," Annual Report: On the Record Briefing. May 21, 2002 <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual Reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

##### SEE ALSO

*Terrorism, Philosophical and Ideological Origins*  
*Terrorist and Para-State Organizations*  
*Terrorist Organization List, United States*  
*Terrorist Organizations, Freezing of Assets*

## OSS (United States Office of Strategic Services)

#### ■ ADRIENNE WILMOTH LERNER

The Office of Strategic Services (OSS) was the first centralized United States intelligence agency. Created in 1942, the agency spearheaded the United States intelligence community, both civilian and military, during World War II. The mission of the OSS was to collect foreign intelligence and sabotage enemy war efforts. Maintaining espionage, analysis, and research forces, the OSS acted as a clearinghouse for information gathered from human and signals intelligence sources. At its peak, the agency employed 13,000 men and women.

Before World War II and the formation of the OSS, the United States employed only small, select intelligence forces within the military. During the American Civil War, a large espionage and intelligence network flourished, but intelligence services were disbanded following the end of the conflict. The military built up its intelligence services

again during the Spanish-American War and World War I. Technological advances in communications, transportation, and weapons in the early twentieth century prompted military commands to continue to operate select intelligence units even during peacetime. The Army maintained its Signals Intelligence Service, a surveillance and cryptanalysis force, and the Navy further developed its intelligence services. Despite the recognition by national leaders that peacetime intelligence was a strategic necessity, the War Department's G-2 Intelligence Division was ill equipped to process, analyze, and disseminate the intelligence information it received from military operations.

The outbreak of World War II in Europe prompted President Franklin D. Roosevelt to press for a more efficient, centralized, and capable national intelligence service. In 1941, with the aid of representatives from the British intelligence community, Roosevelt and his advisors drafted a plan for the creation of new United States intelligence community. William J. Donovan was appointed to act as Coordinator of Information (COI), a civilian office responsible for collating intelligence information and reporting significant discoveries to the President.

When the United States entered the war in 1941, after the bombing of Pearl Harbor, Donovan seized the opportunity to promote the value of the COI and push for an expanded role for his growing intelligence service. The organization was placed under the administration of the Joint Chiefs of Staff, though it remained largely autonomous. The Office of War Information assumed some COI duties, including the government's "white," or attributable, overseas propaganda campaign. Clandestine operations remained in Donovan's control, and his agency was renamed the Office of Strategic Services.

In 1942, the OSS began operations abroad, aiding the Allied war effort in Europe and North Africa. The first major success of the OSS was Operation Torch, a network of agents and informants operating under diplomatic cover in North Africa. Torch operatives reported on German diplomatic relations in the region, as well as troop movements, and strategic battle plans. Torch then contributed key information to Allied command's plans to invade North Africa.

As OSS operations grew more extensive, the agency created specialized operational departments. Though each department conducted independent missions, they worked closely together and had to report at all times to Donovan and other OSS leaders. The most famous of these operational departments was the human intelligence network, the Secret Intelligence Branch (SI). The SI was led by Whitney H. Shepardson and maintained espionage networks in Europe, Asia, and the Middle East.

The mission of the SI created much of the operations doctrine and tradecraft practiced in modern espionage. In 1942, station chief Allen Dulles created one of the most successful units of the SI. Incorporating refugee members of the former French intelligence service who fled the Nazi

occupation of France, Dulles established a network of agents, based in Switzerland, who infiltrated Nazi strongholds and government offices throughout Europe. The SI group provided Allied military command with warnings and information about German V-1 and V-2 missile programs, and later aided the failed attempt by leading German Abwehr agents to assassinate Hitler in 1944. In 1945, Dulles's group of agents, in an operation called Sunrise, helped to secretly broker the surrender of German forces in Italy.

The Special Operations Branch (SO) was the special action force of the OSS. Modeled after the British SOE intelligence group with which it worked, the SO trained intelligence and military officers to aid Resistance groups in France. The SO and SOE created specialized infiltration teams to help organize anti-Nazi groups and assist partisans with weapons and communications equipment. The Jedburghs, as the groups of special SO and SOE agents became known, parachuted in behind enemy lines to coordinate Resistance sabotage efforts. Their mission was to strengthen partisan groups, distract Nazi troops, break enemy supply lines, and aid the Allied invasion forces. The Jedburgh groups achieved their goals with notable success. After the Allied invasion of Normandy in 1944, Jedburghs helped train Resistance members with whom they worked to fight alongside the Allied forces.

Although the espionage-based departments of the OSS gained greater notoriety, the agency's Research and Analysis Department (R&A) was a wholly novel contribution to modern espionage. R&A, comprised of leading academic professors, scientists, engineers, and research specialists in various fields, composed reports using available information to aid covert and military operations. R&A's gathered information about Germany's fuel resources, refineries, and distribution structures. The information allowed Allied airplanes to bomb critical oil production and storage targets, crippling the Nazi war effort. Information about German factories, railroads, and financial networks also contributed to Allied military policy.

Despite the successes and valuable contributions of the OSS, the agency was sometimes limited in its effectiveness. Months after the agency's inception, the government denied the OSS access to enemy communications intercepts and banned it from staffing its own cryptologists to decipher enemy radio and telegraph messages. Fleet commanders in the Pacific rarely utilized OSS forces, and the agency's role in the war against Japan was minimal. The FBI and Naval Intelligence blocked the OSS from extensive domestic counterintelligence work, despite the success of the OSS X-2 strategic counterintelligence network that operated overseas. As a result of its limited participation in routine, domestic defense operations, the OSS came to be seen as a wartime office, a significant factor in its ultimate demise.

Following the end of World War II in 1945, the United States government conducted a wide-scale audit of wartime agencies. The review process was followed by a



massive government restructuring effort, phasing out wartime offices, and incorporating their duties into new agencies. The OSS was disbanded in 1945. Within two years, amid escalating Cold War tensions, the need for a centralized peacetime intelligence service became apparent. The Central Intelligence Agency (CIA) assumed many of the duties of the former OSS.

#### ■ FURTHER READING:

##### BOOKS:

Aldrich, Richard J. *Intelligence and the War Against Japan: Britain, America and the Politics of Secret Service*. Cambridge University Press, 2000.

Bank, Aaron. *From OSS to Green Berets: The Birth of Special Forces*. Novato, CA: Presidio Press, 1986.

Katz, Barry M. *Foreign Intelligence: Research and Analysis in the Office of Strategic Services, 1942–1945*. Cambridge, MA: Harvard University Press, 1989.

##### ELECTRONIC:

Central Intelligence Agency. *The Office of Strategic Services: America's First Intelligence Agency*. <<http://www.cia.gov/cia/publications/oss/>> (1 March 2003).

##### SEE ALSO

*CIA (United States Central Intelligence Agency)*  
*CIA, Formation and History*  
*Cold War (1945–1950), The start of the atomic age*  
*KGB (Komitet Gosudarstvennoi Bezopasnosti, USSR Committee of State Security)*  
*World War II*

*This page intentionally left blank*



## P-3 Orion Anti-Submarine Maritime Reconnaissance Aircraft

First used in the early 1960s, the P-3 Orion was the leading aircraft for United States Navy maritime and anti-submarine reconnaissance over the course of nearly four decades. Many of these aircraft were modified for the collection of electronic intelligence, or ELINT. In 1998, an aging P-3 fleet went through renovations, returning to the skies in the form of the EP-3E Aries. The latter would become involved in an infamous incident involving U.S. reconnaissance over China, a task to which the P-3 had once been deployed.

Replacing the P2V Neptune, the P-3, originally designated P3V, was built by Lockheed and based on the design of the L-188 Electra passenger airliner. The only external differences between the Orion and the Electra were the unpressurized weapons bay forward of the wing, the shorter fuselage, and the magnetic anomaly detector or MAD, a security device, on the tail. Excellent at short takeoff and general handling, the P-3 could readily be modified for the purposes of gathering ELINT. In the latter capacity, it was equipped with direction finders, radar signal analyzers, and other systems.

The first operational flight of the P-3 took place during the Cuban Missile Crisis in October 1962, and during the Vietnam War, several squadrons of P-3s monitored North Vietnamese boats as part of Operation Market Time. In 1963, the Central Intelligence Agency (CIA) converted three P-3As into reconnaissance platforms for use against the People's Republic of China, and these were deployed with Republic of China Air Force markings.

During the 1980s, the U.S. Customs Service began using the P-3 to combat drug trafficking. In 1998, the Navy began updating its aging P-3s, and from these efforts emerged the EP-3E, an airborne radar platform. On April 1, 2001, a Navy EP-3E with a crew of 24 (22 navy personnel, as well as an air force officer and a marine) collided with a Chinese fighter jet off the China coast. The Chinese pilot was killed in the crash, and the damaged U.S. plane landed on nearby Hainan Island. The administration of President George W. Bush called for the immediate return of the plane and crew, but the Chinese ended up holding them for 11 days.

### ■ FURTHER READING:

#### BOOKS:

Bishop, Chris, ed. *The Encyclopedia of Modern Military Weapons: The Comprehensive Guide to over 1,000 Weapon Systems from 1945 to the Present Day*. New York: Barnes & Noble, 1999.

Bonds, Ray, ed. *The Modern U.S. War Machine: An Encyclopedia of American Military Equipment and Strategy*. New York: Military Press, 1987.

#### PERIODICALS:

"Hainan Incident Increases Pressure in Sino-U.S. Relations." *Defense Daily International* 1, no. 2 (April 6, 2001): 14.

"Upgrades for P-3s to Begin in 1998." *Aviation Week & Space Technology* 146, no. 13 (March 31, 1997): 33.

#### SEE ALSO

*E-2C Reconnaissance Ships Designed for Intelligence Collection SIGINT (Signals intelligence) Undersea Espionage: Nuclear vs. Fast Attack Subs*



A U.S. Navy aviation systems warfare operator searches for and tracks surface contacts using radar and the Infrared Detection System of his P-3 Orion patrol aircraft during a routine flight in support of Operation Enduring Freedom in October 2001. AP/WIDE WORLD PHOTOS.

## Pacific Northwest National Laboratory

Since 1965, the Pacific Northwest National Laboratory (PNNL) has been managed by Battelle corporation. Beginning in the 1980s PNNL has operated as a part of the U.S. Department of Energy's national laboratory system—adding the term “National” to its name in 1995—and Battelle now manages the site for the Department of Energy's Office of Science. PNNL scientists and engineers conduct basic science research, joint research projects with private industry, and specialized research related to national security issues.

Although initially founded to conduct research work related to the Hanford nuclear site in Washington State—including the development of technology to improve safety in fabricating and handling nuclear fuels—research has since expanded to encompass an interdisciplinary approach to environmental, biotechnology, computer science, and national security related projects.

Of historical interest, PNNL scientists assisted NASA scientists in the analysis of materials collected during

Apollo lunar exploration missions. PNNL studies included measurements of radionuclides that provided evidence of not only lunar processes, but of solar processes not easily measured in Earth materials. Other PNNL historical achievements include the development of optical digital recording technologies used in preparing compact discs.

In an attempt to address the growing need for finding safer modes of hazardous waste disposal, PNNL scientists developed the process of vitrification (a process that encases hazardous waste in a stable glass matrix that can then be safely stored for thousands of years). Expanding on its history in developing hazardous waste technology, more recent PNNL projects have developed new methodologies to handle nuclear tank waste often stored in deteriorating and vulnerable underground tanks. Clean up and the development of protocols for handling contaminated materials focuses on preventing radionuclide loss or other hazardous material contamination of the surrounding environment. As part of environmental research programs, PNNL scientists have developed sophisticated global climate models that allow researchers to predict the global atmospheric spread of hazardous materials or the movement of hazardous wastes through groundwater systems. PNNL-developed technology assists monitoring of nuclear testing ensures adherence to the Comprehensive (Nuclear) Test Ban Treaty (CTBT).



A senior research engineer at the Pacific Northwest National Laboratory conducts a tour of the napalm canister separation plant located at the Naval Weapons Station Seal Beach Detachment in 2001. After a two-year effort, the Navy disposed of more than 34,000 napalm bombs that sat for more than a quarter of a century on fields surrounding the facility. AP/WIDE WORLD PHOTOS.

PNNL's Chemical and Biological Defense Program is continuing research into detection technologies capable of identifying prohibited chemical and biological agents. PNNL technologies that facilitate pathogen detection include the Matrix-Assisted Laser Desorption/Ionization Mass Spectrometry (MALDI-MS) program that utilizes mass spectrometry to rapidly identify pathogens. Instead of conventional bio-identification procedures that can take days of laboratory analysis time—and thus, delay effective response to acts of bioterrorism—MALDI-MS holds the potential to allow pathogen identification within minutes. For example, the Biodetection Enabling Analyte Delivery System (BEADS) analyzes microbe DNA for pathogen identification. In conjunction with private industry, PNNL projects include the development and evaluation of systems to effectively distribute enzymes and chemicals that decontaminate a structure following chemical or biological agent exposure.

In partnership with U.S. Department of Energy's Hazardous Materials Management and Emergency Response

(HAMMER), PNNL staff offers training to law enforcement officers, emergency medical responders, and military personnel in methods of managing responses to potential nuclear, chemical, or biological accidents and deliberate acts of terrorism.

To support inspection efforts—such as those conducted by U.N. weapons inspectors in Iraq prior to the 2003 U.S.-led war against Iraq—PNNL scientists developed acoustic inspection devices that were capable of detecting compartments inside liquid-filled containers.

Other PNNL projects related to national security include a holographic imaging system that enhances non-invasive personal screening for use by the Federal Aviation Administration.

#### ■ FURTHER READING :

##### ELECTRONIC:

Pacific Northwest National Laboratory. March 2003. <<http://www.pnl.gov/>> (April 2, 2003).

United States Department of Energy, Office of Science. National Laboratories and User Facilities. <[http://www.sc.doe.gov/Sub/Organization/Map/national\\_labs\\_and\\_userfacilities.htm](http://www.sc.doe.gov/Sub/Organization/Map/national_labs_and_userfacilities.htm)> (March 23, 2003).

United States Department of Homeland Security. Research & Technology. <<http://www.dhs.gov/dhspublic/display?theme=27&content=374>> (March 23, 2003).

#### SEE ALSO

*Argonne National Laboratory*  
*Brookhaven National Laboratory*  
*DOE (United States Department of Energy)*  
*Environmental Measurements Laboratory*  
*Lawrence Berkeley National Laboratory*  
*Lawrence Livermore National Laboratory (LLNL)*  
*Los Alamos National Laboratory*  
*NNSA (United States National Nuclear Security Administration)*  
*Oak Ridge National Laboratory (ORNL)*  
*Plum Island Animal Disease Center*  
*Sandia National Laboratories*

---

## Pakistan, Intelligence and Security

---

In 1947, the British ended their colonial control of the Indian subcontinent. British India was divided into two sovereign states, predominantly Hindu India and Muslim Pakistan. A war in 1971 further divided the region, creating the nation of Bangladesh. The division sparked endemic strife in the region, especially in the ethnically diverse Kashmir province. Tensions over Kashmir, water rights of the Indus River, and occasional armed conflict continue to plague Pakistan and India.

Conflict in the region escalated in the late 1990s when India began extensive nuclear weapons testing near the Pakistani border. In 1998, Pakistan began a nuclear weapons program. Western nations, including the United States, are concerned not only with the possibility of dueling nuclear powers on the Indian subcontinent, but also with the possible proliferation of nuclear materials and technology to neighboring nations and terrorist organizations. Pakistan's intelligence services are suspected of playing a crucial role in the country's nuclear program, both securing nuclear materials and conducting espionage on other nuclear programs.

Pakistan's intelligence community is divided into three main agencies. The agencies are neither wholly civilian, nor wholly military, and their duties in foreign and domestic intelligence often overlap. Inter-Services Intelligence (ISI) is the premier Pakistani intelligence and security organization. The ISI collects domestic and foreign intelligence, focusing especially on surveillance of foreign diplomats operating within Pakistan. No government or military body oversees the actions of the ISI, which has led to

the agency gaining significant power. The ISI monitors communications, maintains a special, military-trained action group, and conducts political espionage.

Various operational divisions within the ISI attend to different aspects of the organization's mission to protect national security. The Joint Signal Intelligence Bureau coordinates communications and signal surveillance operations. The Joint Counter Intelligence Bureau monitors Pakistani diplomats serving abroad and conducts counter-espionage operations. Assessing threats to national security and collating intelligence data is the primary responsibility of the Joint Intelligence X.

The Intelligence Bureau (IB) is Pakistan's main domestic intelligence and espionage agency. The IB conducts political surveillance of politicians, government agents, businesses, and citizen groups. Political surveillance is used to identify and infiltrate groups that the Pakistani government considers hostile or anti-government. Although the agency has no formal arrest powers, suspects are often arrested and detained by law enforcement at the request of IB officials. In 1996, the IB was granted control of government censorship programs, controlling information dissemination via mail, wire, or electronic medium.

The Pakistani government has been dominated by military forces for decades. The election of some moderate leaders in 2000 led to minor demilitarization reforms within the government. In subsequent elections, Islamist hardliners gained seats in Pakistan's parliament, effectively halting impending reforms. A reflection of the government, the Pakistani intelligence community is also a mix of military and civilian forces. Military Intelligence (MI) performs the same duties as its government agency counterpart, conducting political surveillance and protecting national security. While the MI is especially concerned with the security of military installations, weapons facilities, and border control, its routine operations are similar to the ISI and IB.

While some reforms have been made to the Pakistani intelligence community, the national government continues to take criticism from the international community on its lack of support for antiterrorism measures in the region. The United States officially warned Pakistan to cease terrorist operations in India in the late 1990s. Following the September 11, 2001, terrorist attacks on the United States, Pakistan again came under the scrutiny of Western nations for its tolerance of terrorist organizations, such as al-Qaeda, operating within its borders. Although Pakistan's leader, General Pervez Musharraf, eventually pledged and lent support to the United States-led coalition in the war against the Taliban in Afghanistan, some Western analysts initially challenged the commitment and loyalties of the Pakistani intelligence service toward the international war on terrorism. Subsequent actions have signaled Pakistan's overt willingness to become a full and active participant in the international war on terrorism. On March 1, 2003, agents of Pakistan's ISI intelligence agency, in cooperation with U.S. CIA operatives tracked down and

arrested Khalid Sheikh Mohammed, the suspected al-Qaeda operations director implicated in a string of terrorist attacks. Pakistan intelligence agents were also instrumental in the prior arrest of another highly placed al-Qaeda terrorist, Abu Zubaida. Both terrorists were turned over to the CIA for interrogation at an undisclosed location.

#### ■ FURTHER READING :

##### BOOKS:

Jaffrelot, Christophe. *A History of Pakistan and Its Origins*. Translated by Gillian Beaumont. New York: Anthem Press, 2002.

Jones, Owen Bennett. *Pakistan: Eye of the Storm*. New Haven, CT: Yale University Press, 2002.

Ziring, Lawrence. *Pakistan in the Twentieth Century: A Political History*. Oxford: Oxford University Press, 1998.

##### PERIODICALS:

Gauhar, Altaf. "How Intelligence Agencies Run Our Politics." *The Nation*. September 1997: 4.

##### SEE ALSO

*India, Intelligence and Security*  
*Nonproliferation and National Security, United States*  
*Weapons of Mass Destruction*  
*Weapons of Mass Destruction, Detection*

## Palestine Islamic Jihad (PIJ)

The Palestine Islamic Jihad (PIJ) originated among militant Palestinians in the Gaza Strip during the 1970s. The PIJ-Shiqaqi faction, currently led by Ramadan Shallah in Damascus, is most active. Committed to the creation of an Islamic Palestinian state and the destruction of Israel through holy war, PIJ also opposes moderate Arab governments that it believes have been tainted by Western secularism.

**Organization activities.** PIJ activists have conducted many attacks including large-scale suicide bombings against Israeli civilian and military targets. The group increased its operational activity in 2001 during the Intifadah, claiming numerous attacks against Israeli interests. The group has not targeted U.S. interests and continues to confine its attacks to Israelis inside Israel and the territories.

The actual number PIJ activists is unknown. The PIJ operates primarily in Israel, the West Bank and Gaza Strip, and other parts of the Middle East, including Lebanon and Syria, where the leadership is based. They receive financial assistance from Iran and limited logistical support from Syria.

##### ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001. Annual Report: On the Record Briefing. May 21, 2002. <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

##### SEE ALSO

*Terrorism, Philosophical and Ideological Origins*  
*Terrorist and Para-State Organizations*  
*Terrorist Organization List, United States*  
*Terrorist Organizations, Freezing of Assets*

## Palestine Liberation Front (PLF)

The Palestine Liberation Front (PLF) broke away from the Popular Front for the Liberation of Palestine-General Command (PFLP-GC) in the mid-1970s. The PLF later split again into pro-PLO, pro-Syrian, and pro-Libyan factions. The Pro-PLO faction is led by Muhammad Abbas (Abu Abbas), who became a member of the PLO Executive Committee in 1984 but left it in 1991.

**Organization activities.** The Abu Abbas-led faction is known for aerial attacks against Israel. Abbas's group also was responsible for the attack in 1985 on the cruise ship *Achille Lauro* and the murder of U.S. citizen Leon Klinghoffer. Following a brief standoff, Egypt granted free passage to the hijackers in exchange for the release of the ship and remaining hostages. The plane carrying the hijackers to refuge in Tunisia was intercepted by U.S. Navy jets and diverted to Italy. Although Abbas's coconspirators were rapidly convicted and sentenced to prison, Abbas was freed by the Italian authorities, who claimed they had insufficient evidence to detain him. Abbas was, however, subsequently convicted in absentia of masterminding the hijacking.

Abu Abbas was found in Baghdad following Operation Iraqi Freedom and as of April 2003, was in U.S. custody. Abbas had been cited by President George W. Bush as an example of terrorists given safe haven by the Saddam Hussein regime. During Operation Iraqi Freedom, U.S. marines found bombmaking equipment, explosives, gas masks, and other weapons at a large PLF training facility east of Baghdad.

The size of the PLF is unknown; the PLO faction was based in Tunisia until the *Achille Lauro* attack, and then in

Iraq until Operation Iraqi Freedom. Prior to the military action in Iraq the PLF received support mainly from Saddam Hussein's regime. The PLF also has received support from Libya.

■ FURTHER READING:

ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001. Annual Report: On the Record Briefing. May 21, 2002. <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

SEE ALSO

*Terrorism, Philosophical and Ideological Origins Terrorist and Para-State Organizations*  
*Terrorist Organization List, United States*  
*Terrorist Organizations, Freezing of Assets*

---

## Palestinian Authority, Intelligence and Security

---

The Israeli-Palestinian struggle has been marked by violence and international diplomatic conflict since the British "Balfour Declaration" opened the predominately Arab territory of Palestine to large-scale Jewish immigration. Tensions escalated in the region, with outbreaks of periodic violence, even before the establishment of the State of Israel in 1947. Israeli territorial expansion in 1948 further angered Palestinians when Jerusalem was declared an Israeli city, violating the original agreement that made the religious seat an international city. The Six Day War in the late 1960s further expanded Israeli control in the region, again sparking violence between the region's factions.

In the 1990s, Israel and the Palestinian Authority began a series of peace talks. However, growing nationalism and radical fundamentalism in both Israel and Palestine undermined the peace process. The Palestinian State claims that Israel continues to occupy Palestinian territory illegally, and Israel says that its military presence is necessary to protect Jewish peripheral settlements. In 2001, a new wave of violence in the region marked the beginning of the second Intifadah. The Palestinian Authority, and its military and intelligence community have been cited by the international community for prolonging the Intifadah and encouraging anti-Israeli and anti-American terrorism.

Little is known about the structure and the daily functions of the Palestinian intelligence and security community. The main intelligence agencies are the National Security Service and General Intelligence. Domestic political intelligence and foreign intelligence (mostly espionage against Israeli defense forces) is carried out by these organizations, which rely on a large network of human intelligence and informants. There is no real distinction between civilian and military intelligence forces, since much of the Palestinian Authority is para-military in nature.

The Palestinian Authority maintains three major security forces. The Presidential Police protect Palestinian officials and provide a special guard to Palestinian leader Yassar Arafat. The Civil Police protect public welfare, and sometimes operate with the military against Israeli forces. The Preventative Security Forces are a quasi-intelligence based, secret police force.

After the terrorist attacks on the United States, Arafat quickly distanced his national forces from those of Al-Qaeda. However, many in the international community remain skeptical, noting Arafat's connection to other Islamist groups. In 2003, the United States government released a "Road Map to Peace," a long-term compromise proposal to halt growing Israeli-Palestinian violence. However, many Palestinians and Israelis disagree on the future prospects of peace in the region, and the nature of any settlement between their two governments, especially in light of the conflict in Iraq. The Palestinian Authority continues its endeavors to gain international support for and recognition of an independent Palestine.

■ FURTHER READING:

ELECTRONIC:

United Nations. "The Question of Palestine." <<http://www.un.org/Depts/dpa/ngo/history.html>> (13 March 2003).

SEE ALSO

*Israel, Intelligence and Security*  
*Terrorism, Philosophical and Ideological Origins*  
*Terrorist and Para-State Organizations*  
*United Nations Security Council*

---

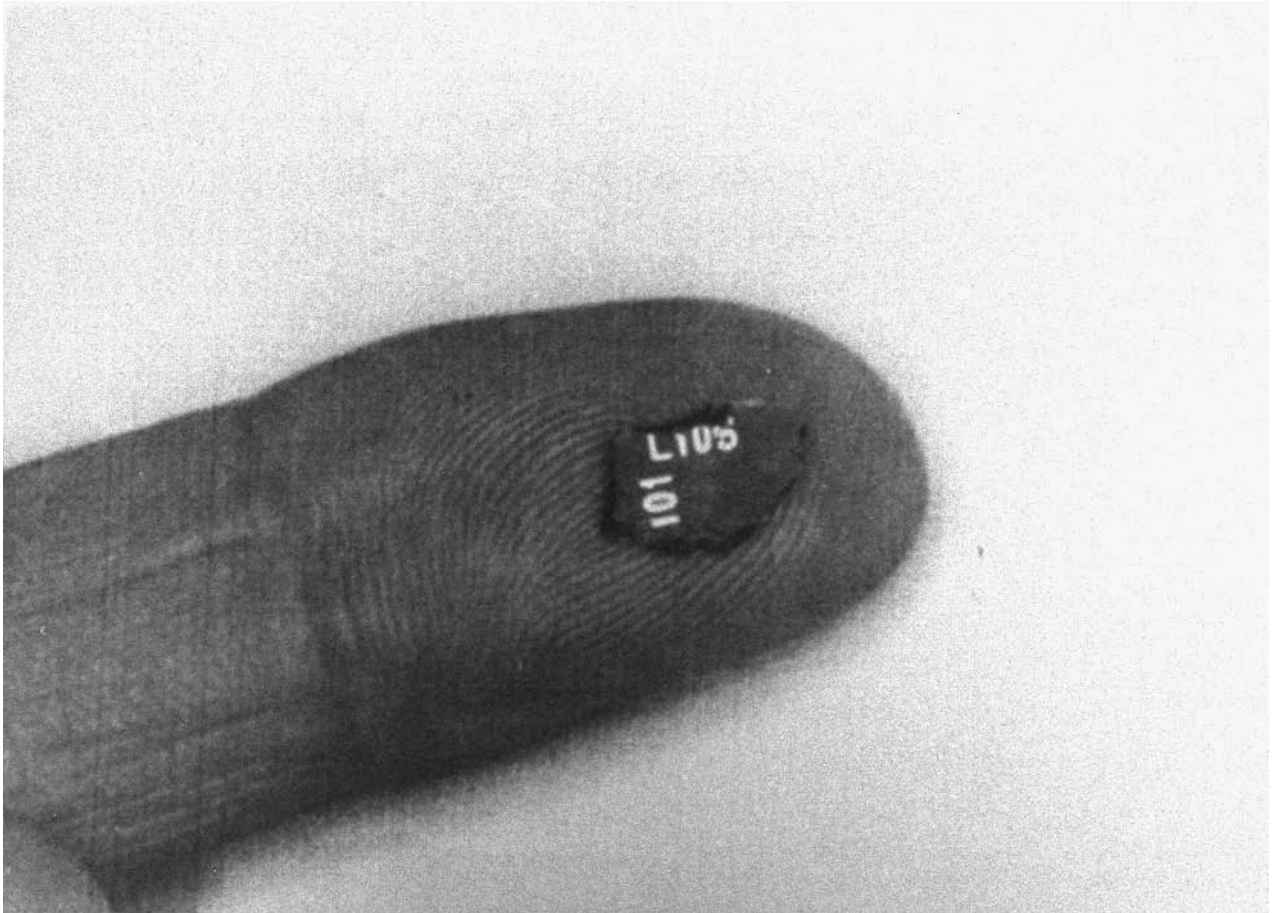
## PanAm 103, (Trial of Libyan Intelligence Agents)

---

■ MICHAEL J. O'NEAL

On December 21, 1988, a bomb planted on PanAm Flight 103 en route to New York exploded while the plane was airborne over Lockerbie, Scotland. After an extensive investigation, two men with alleged ties to the intelligence service of Libya were extradited and brought to trial. In





One of two fragments that proved crucial in tracking down the bombers of PanAm Flight 103, which exploded over Lockerbie, Scotland, in 1988, is shown on the tip of a finger. AP/WIDE WORLD PHOTOS.

January 2001, one of the accused was found guilty and sentenced to life in prison; the other was acquitted.

**Background.** PanAm Flight 103, which originated in Frankfurt, Germany, took off from London's Heathrow Airport at 6:25 PM on December 21, 1988. The flight path of the plane was to take it over the British Isles and the North Atlantic Ocean on its way to New York City. At 6:56 PM the plane leveled out at 31,000 feet. Seven minutes later, the air traffic controller at Shanwick Oceanic Control transmitted the plane's final oceanic clearance but received no acknowledgment from the aircraft. During the transmission, the plane's radar return disappeared from controller radar screens.

What air traffic controllers and others later learned was that at 7:02 and 50 seconds, the Boeing 747 exploded in midair over Scotland, killing all 259 passengers and crew members aboard. The bulk of the wreckage hit a residential area called Sherwood Crescent at the southern edge of the town of Lockerbie, digging a crater 155 feet wide and 196 feet long, destroying 21 residential buildings, and killing 11 people on the ground. The impact of

the crash was so strong that the British Geological Survey reported what appeared to be an earthquake registering 1.6 on the Richter scale. Other parts of the plane fell into the countryside east of town, but investigators later discovered bits of wreckage as far away as 80 miles. Within hours, journalists flooded the scene and transmitted the first pictures of the smoking wreckage.

**The investigation.** Responsibility for determining the cause of the crash fell to the United Kingdom's Air Accident Investigation Branch (AAIB). The AAIB quickly began the task of painstakingly reassembling the nearly four million pieces of wreckage recovered, often having to sift through bags of mud and debris to find them. After reconstructing the plane, the investigators determined that the cause of the catastrophe was an explosion, which in turn was caused by a so-called IED, or "intentional explosive device."

The PanAm 103 investigation focused on a Toshiba radio/cassette recorder that had been packed into a brown suitcase stowed in the cargo hold of the plane. Inside the

recorder were the remains of a timing device that detonated the bomb. The central question, of course, was the identity of the person or persons who planted the bomb.

There was no shortage of theories. Families of many of the victims publicly tied the explosion to the government of Iran, claiming that Iranian hard-liners were bent on vengeance for an incident in July 1988 when the U.S. Navy cruiser *Vincennes* accidentally shot down an Iranian plane with 290 passengers aboard. Others pointed a finger at the Palestinians, for the barometric timing device that detonated the bomb matched similar devices found during an October 26, 1988 raid by German police on two apartments occupied by members of the Popular Front for the Liberation of Palestine. There they found a virtual bomb factory complete with timers, barometric devices, explosives, detonators, and Toshiba radio/cassette recorders.

**The Libyan connection.** In November 1991, after a three-year investigation, Scotland's chief law enforcement officer issued warrants for the arrest of two Libyans. One was Al-Amin Khalifa Fhimah, an alleged member of the Libyan Intelligence Services and the station officer of Libyan Arab Airlines on the Mediterranean island of Malta. The other was Abdel Baset al-Megrahi, alleged to have been a senior officer in the Libyan Intelligence Services and head of Libyan Airlines security.

It was one thing to issue warrants. It was another matter entirely to extricate the suspects from Libya, a north African nation ruled by Colonel Muammar Gaddafi. The United States had long identified Gaddafi's Libya as a "rogue" state, and Gaddafi never attempted to hide his virulent anti-Western sentiments. Tensions between Gaddafi and the United States came to a boil in March 1986, when Libya attacked a fighter aircraft of the U.S. Sixth Fleet, which was on maneuvers in the Mediterranean. The United States retaliated by bombing Libyan radar and missile installations. Then in April, a bomb in a Berlin discotheque killed an American soldier and a Turkish woman. The United States had evidence that Libya was behind the bombing and in retaliation attacked military and civilian targets in the Libyan capital of Tripoli, including Gaddafi's residence.

Against this backdrop, Gaddafi argued for nearly eight years that the suspects could not receive a fair trial in a Scottish court. In spite of sanctions by the United Nations that eventually cost Libya an estimated \$33 billion, Gaddafi refused to extradite the suspects until 1998, after UN Secretary General Kofi Annan and South African leader Nelson Mandela intervened, possibly offering assurances that Gaddafi himself would be granted immunity from prosecution for the crime. Authorities agreed to Gaddafi's condition that the trial be conducted in a neutral third country. Accordingly, in 1998 the Netherlands agreed to set aside Camp Zeist, a former air base, as the site of the trial, complete with an \$18 million courtroom constructed with bulletproof glass.

The trial attracted worldwide attention because of its international implications. The prosecution argued that the men had acted under the orders of Gaddafi himself, whose motive was revenge for the 1986 bombing raid on Tripoli that killed his daughter. The defense countered that the real perpetrators were an extreme militant faction of the Popular Front for the Liberation of Palestine with help from the governments of Iran and Syria. In its verdict, announced in early 2001, the three-judge panel of Scottish judges did not address these wider issues. Based on over 10,000 pages of testimony from 235 witnesses, the panel found Fhimah not guilty because the prosecution was never able to establish that he was at the airport in Malta when he was alleged to have used his position to get the bomb on a plane bound for Frankfurt.

In convicting al-Megrahi, however, the court focused on a number of pieces of evidence. On December 20, 1988, al-Megrahi had traveled to Malta under a false name. There, according to a Maltese shop owner, he purchased clothes, but he did not seem to be very interested in what clothes he was buying. The clothes and the bomb were placed aboard an Air Malta flight to Frankfurt, where they were transferred to Flight 103. While the shop owner was never able positively to identify al-Megrahi, bits of the clothing he purchased were found with the Toshiba cassette parts recovered in Scotland. Finally, al-Megrahi had a close association with Edwin Bollier, an electronics expert from Zurich, Switzerland, who, prosecutors said, had manufactured the timer for the bomb. With regard to the timer, though, some observers continue to have questions. The timer that prosecutors said detonated the bomb was sophisticated enough that it could have been set to detonate when the plane was over the Atlantic. Doing so would have thwarted investigators in their efforts to recover debris and track down the bombers. Cruder timers, though, could be set for no longer than 45 minutes, within the time frame when the bomb exploded. This led some to wonder whether the Toshiba fragments prosecutors produced in evidence were really parts of the timer that detonated the bomb.

Al-Megrahi's conviction did not settle the case. Some of the victims' families continued to insist that Iran played a role in the bombing. Others continued to call for prosecution of al-Megrahi's superiors, including Gaddafi himself. Civil suits for damages against the Libyan government are likely to continue for years. In 2021, al-Megrahi will be eligible for parole.

#### ■ FURTHER READING:

##### BOOKS:

- Cohen, Susan, and Daniel Cohen. *Pan Am 103: The Bombing, the Betrayals, and the Bereaved Families' Search for Justice*. New York: Signet, 2001.
- Emerson, Steven, and Brian Duffy. *The Fall of Pan Am 103*. New York: Putnam, 1990.
- Gerson, Allan, and Jerry Adler. *The Price of Terror*. New York: HarperPerennial, 2002.

House Committee on Foreign Affairs. *U.S. Policy in the Aftermath of the Bombing of Pan Am 103*. Hearing before the Subcommittees on International Security, International Organizations, and Human Rights. 103rd Cong., 2nd sess., July 28, 1994.

#### PERIODICALS:

“Case Closed?” *Time International*. February 12, 2001: 16ff.

#### ELECTRONIC:

Morse, Amanda, and Derek Brown. “The Lockerbie Trial.” *The Guardian*. January 31, 1997. <<http://www.guardian.co.uk/theissues/article/0,6512,216784,00.html>>.

#### SEE ALSO

*Airline Security*  
*Bomb Damage, Forensic Assessment*  
*Libya, Intelligence and Security*  
*Terrorist Organization List, United States*

## Panama Canal

■ JUDSON KNIGHT

From the time of its opening in 1914 until 1977, when the United States transferred it to the nation of Panama, the Panama Canal was a symbol of U.S. influence in the Americas and, ultimately, the world. Despite the bitterness that attended the debate over its transfer to Panama, combined with fears of foreign takeover that surfaced when Panama took formal control on December 31, 1999, the Canal lacks the strategic importance it enjoyed in its heyday. Still, it remains one of several important “chokepoints”—areas in which the flow of the world’s oil supply traverses a narrow passage vulnerable to attack—and for this reason, the United States remains committed to the Canal’s defense.

### Early history

From the earliest voyages of discovery in the area of Central America and the Caribbean, it became clear that a canal across one of Central America’s narrowest points would greatly shorten travel and transport time between Atlantic and Pacific ports. In 1835, the U.S. Senate passed a resolution in favor of building such a canal, but through Nicaragua. In 1881, a French team under the leadership of Ferdinand de Lesseps, builder of the Suez Canal, attempted to build a canal across the isthmus of Panama, but the project suffered a number of misfortunes, including bankruptcy and outbreaks of disease among workers. The French project was scrapped for good in 1898.

Meanwhile, the idea of a canal remained a topic of debate in the United States, which still favored a route

through Nicaragua. After much political wrangling, however, Congress in 1902 passed the Spooner Act, which authorized the United States to purchase the assets of the French company and begin building a canal through Panama. The latter at that time belonged to Colombia, and when treaty negotiations with Colombia stalled, U.S. authorities gave their support to a declaration of independence by Panama in November 1903. Colombia, convulsed by four years of civil war, could do little to stop the act of secession, and the United States completed a treaty with the new nation of Panama. In February 1904, Congress created the Panama Canal Zone.

The building of the Canal took place over a 10-year period beginning in the summer of 1904. Its builders, who numbered as many as 40,000 at any one time, consisted of American and European engineers and technicians, with Latin American and Chinese immigrant labor. Among the challenges they confronted were disease, carried by mosquitoes that lived in the swampy lands along the canal route, and topography. Rather than build at sea level, the engineers finally decided on a plan involving a series of locks and an earthen dam, which created what was then the world’s largest artificial lake, Gatun. The Canal—which actually follows a route from the northwest to the southeast, rather than east to west—opened on August 15, 1914.

### Rethinking the Canal

Although the Canal was a vital lifeline during the two world wars, by the time of the Korean War, its limitations had begun to show. The Canal could not accommodate very large aircraft carriers, an increasingly critical aspect of U.S. national security. By the mid-1970s, most large oil tankers were also too big for passage.

Coupled with the physical issues were political ones associated with the growth of anti-American sentiment in Panama and elsewhere. On January 9, 1964, American refusal to fly the Panamanian flag over a high school in the Canal Zone sparked riots that left 23 Panamanians and four U.S. Marines dead. Afterward, Panama called for new treaty discussions with the United States.

**The treaties.** On September 7, 1977, President James E. Carter and Panamanian military dictator Omar Torrijos signed the Panama Canal Treaty, which abolished the Canal Zone, terminated all prior treaties regarding the Canal, and provided for the full transfer of the Canal to Panama on December 31, 1999. A separate Neutrality Treaty guaranteed the neutrality of the Canal in perpetuity.

The Neutrality Treaty and several aspects of the Panama Canal Treaty served to protect U.S. interests—interests that, in the view of many Treaty supporters, were best supported by a voluntary transfer of the Canal. The alternative, supporters maintained, would be a political and public-relations disaster for the United States, and would only serve to bolster Latin American resentment against the wealthy, powerful neighbor to the north.



As ten percent of the world's ships are unable to pass through the strategic Panama Canal waterway, the canal is undergoing its largest expansion since workers carved the 50-mile path through Panama's mountains, linking the Pacific and Atlantic oceans. AP/WIDE WORLD PHOTOS.

Opponents to the Canal agreements, led by future President Ronald Reagan, cited the Treaty as one further sign of America's worldwide retreat, and warned of foreign takeover. Nevertheless, the transfer plan enjoyed support from a number of Republicans, including former President Gerald R. Ford and former Secretary of State Henry Kissinger. In 1978, the Senate ratified both treaties, and in 1979 Congress passed the Panama Canal Act. Among its many provisions, the Act created the Panama Canal Commission, which would act as custodian over the Canal for the next 20 years.

**The transfer.** Panama has not fared well in the years since the Treaty. The United States deposed another dictator, Manuel Noriega, in 1989, acting partly to protect the Canal from takeover. The country has been run by civilian governments since then, but these have proven inadequate to solve the nation's domestic problems. As the December, 1999, deadline loomed, some Panamanians expressed reservations regarding the transfer of the Canal.

On the one hand, its acquisition would greatly enhance national prestige, but many wondered if any small, poor country could undertake an operation hitherto overseen by the world's leading superpower. Similar concerns

in the United States led to a proposal regarding a continued U.S. military presence. However, talks between the two nations ended in September, 1998, without any such agreement.

On the last day of the 1900s, U.S. Army Secretary Louis Caldera led a delegation that officially turned over control of the Canal to Panama, represented by President Mireya Moscoso. Minutes before the hoisting of the Panamanian flag over the Canal administration building, a triumphant Moscoso proclaimed to her people, "The Canal is ours!"

## The Canal Today

Subsequent events have not served to reinforce this initial enthusiasm. The Canal has faced several environmental problems, including a lack of rainwater, important to the transport of ships through its 12 locks, caused by droughts resulting from the El Niño weather phenomenon. Political and economic corruption has also shadowed the Canal. Not only did a local land-sale scam involving Canal properties bilk investors, but in November, 2000, it was discovered that millions of dollars in U.S. equipment (including firearms) from the former Canal Zone had disappeared.

Some of the fears raised prior to the transition, however, have proven illusory. One was the question of Chinese control, a powerful issue in Washington due to allegations of widespread Chinese espionage against the United States during the administration of President William J. Clinton. When the Hong Kong conglomerate Hutchison-Whampoa gained a contract to manage ports on the Atlantic and Pacific sides, this raised concerns that the Chinese might use this as an opportunity to seize control of the Canal. Subsequent events, however—or rather, the lack of events in this regard—have served to support the view of those who pointed out that China has never been expansionist beyond Asia.

If the Canal faces a serious foreign threat, it is likely to come from much closer to home, such as from Colombia, which continually teeters on the brink of anarchy as its government battles drug traffickers, revolutionaries, and paramilitary groups. At the beginning of the twenty-first century, many international observers expressed grave concerns that Panama in general, and the Canal in particular, could be drawn into these struggles.

In any case, the Canal lacks the strategic significance it once held, and in 2000 only 1.7 percent of total U.S. petroleum imports passed through it. Though as many as 10,000 vessels navigate the Canal each year, traffic has declined since the peak year, 1970, and today 10 percent of the world's cargo ships are too large to traverse it. Additionally, the Trans-Panama Pipeline, opened in October 1982, could be used to ship oil across the Panamanian isthmus if the Canal were closed. Discussions regarding an enlarged or alternate canal are ongoing, though it is unlikely such a project could be undertaken without a wealthy nation or nations to underwrite it.

#### ■ FURTHER READING :

##### BOOKS:

- Collin, Richard H. *Theodore Roosevelt's Caribbean: The Panama Canal, the Monroe Doctrine, and the Latin American Context*. Baton Rouge: Louisiana State University Press, 1990.
- Falcoff, Mark. *Panama's Canal: What Happens When the United States Gives a Small Country What It Wants*. Washington, D.C.: AEI Press, 1998.
- Leonard, Thomas M. *Panama, the Canal, and the United States: A Guide to Issues and References*. Claremont, CA: Regina Books, 1993.
- Major, John. *Prize Possession: The United States and the Panama Canal, 1903–1979*. New York: Cambridge University Press, 1993.
- Strong, Robert A. *Working in the World: Jimmy Carter and the Making of American Foreign Policy*. Baton Rouge: Louisiana State University Press, 2000.

##### SEE ALSO

*Americas, Modern U.S. Security Policy and Interventions Carter Administration (1977–1981), United States National Security Policy*

*Clinton Administration (1993–2001), United States National Security Policy*  
*Suez Canal*

## Parabolic Microphones

■ LARRY GILMAN

A parabolic microphone is an ordinary microphone mounted inside a sound-reflecting dish having a parabolic cross section. Sound waves passing straight into the parabolic reflector are focused by it on the microphone; sounds entering the reflector dish from other angles impinge directly on the microphone, but are not focused on it by the reflector. Thus, the parabolic microphone is highly directional, that is, more sensitive to sound sources at which it is directly pointed than to other sources. This makes the parabolic microphone useful for recording localized sources of relatively faint sounds, such as conversations or bird calls, at a distance.

A paraboloid reflector is used because of the unique geometrical properties of the parabola. A parabola is an open curve resembling a V with a rounded point. (Mathematically, the two arms of the curve go on forever; in building a parabolic reflector, the arms are cut short.) The “axis” of the parabola is a straight line that passes through it like a vertical line drawn through the center of a V. All rays that enter a parabola parallel to its axis and are reflected from the curve (like light rays from a mirror) pass through a single point inside the parabola, the focus. In a parabolic microphone system, the microphone is placed at this point; sound waves entering the dish parallel to the axis are focused on the microphone and, thus, amplified.

Another type of directional microphone, the shotgun mike, attains directionality by embedding the microphone in a long, narrow, open-ended tube; only sound approaching the mike along the axis of the tube can reach the mike. On one hand, the shotgun design does not *focus* sound on the mike, and so is not as sensitive as the parabolic design; on the other, the shotgun mike is less cumbersome and less open to off-axis sounds.

Parabolic reflectors are also used to create light beams from point sources. All light emanating from a point source placed at the focus of a parabolic reflector will exit the reflector in the direction of the parabola's axis. (The bulbs of car headlights are placed at the foci of parabolic reflectors.)

#### ■ FURTHER READING :

##### ELECTRONIC:

Weisstein, Eric W. “Parabola.” MathWorld (Wolfram Research). <<http://mathworld.wolfram.com/Parabola.html>> (April 17, 2003).

## Pathogen Genomic Sequencing

The Pathogen Genomic Sequencing program initiated by the Defense Advanced Research Project Agency (DARPA) in 2002 focuses on characterizing the genetic components of pathogens in order to develop novel diagnostics, treatments and therapies for the diseases they cause. In particular, the program will collect an inventory of genes and proteins that are specific to pathogens and then look for patterns among these molecules. This information will facilitate the development of tools for identifying pathogens in a variety of vectors. It will also provide a foundation for engineering antibodies to identify pathogens. Initially, one representative strain of the bacteria that cause a variety of diseases (or their close relatives) are being studied for this program: *Brucella suis* (brucellosis), *Burkholderia mallei* (melioidosis), *Clostridium perfringens* (botulism), *Coxiella burnetti* (Q fever), *Francisella tularensis* (tularemia), and *Rickettsia typhi* (Rocky Mountain spotted fever).

As part of the Pathogen Genomic Sequencing project, a website focusing on orthopox viruses has been created. Known as the Poxvirus Bioinformatics Resource, this website serves as a repository for genetic sequence data for orthopox viruses. It currently contains sequence data for 35 viral pathogens including the virus that causes smallpox. In addition, the website contains data-mining and sequence analysis software and a poxvirus literature resource. The goals of the Poxvirus Bioinformatics Resource are the development of novel therapies for human diseases caused by orthopox viruses, the ability to detect orthopox viruses in the environment and the development of quick diagnostic tools for detecting pox diseases.

### ■ FURTHER READING:

#### ELECTRONIC:

Defense Advanced Research Projects Agency. Defense Sciences Office. "Pathogen Genomic Sequencing." <<http://www.darpa.mil/leaving.asp?url=http://www.poxvirus.org>> (April 1, 2003).

Poxvirus Bioinformatics Resource Center. <<http://www.poxvirus.org/>> (April 1, 2003).

#### SEE ALSO

*DARPA (Defense Advanced Research Projects Agency) Pathogens*

other species. Pathogen transmission involves three steps: escape from the host, travel to, and infection of the new host. Pathogen transmission occurs in several ways, usually dependent on the ecology of the organism. For example, respiratory pathogens are usually airborne, while pathogens of the digestive tract tend to occur in food or water. Epidemiologists group pathogen transmission into two general types of contact, direct and indirect, within which there are several mechanisms.

Pathogen transmission by direct contact takes place when an infected host transmits a disease directly to another host. The pathogens that travel this way are extremely sensitive to the environment and cannot be outside of the host for any length of time. For example, pathogens that cause sexually transmitted diseases (STDs) are transmitted via blood, semen, or saliva. Some pathogens responsible for STDs include *Tremonema palidum* (syphilis), *Neisseria gonorrhoeae* (gonorrhea), and the pathogen that causes Acquired Immunodeficiency Syndrome or AIDS, Human Immunodeficiency Virus (HIV). The viruses responsible for hemorrhagic fever, such as Ebola, are also transmitted by direct contact via the blood.

Indirect transmission occurs when an agent is required to transfer the pathogen from an infected host to a susceptible host. The agent may be either animate or inanimate. Animate transmission agents, which are referred to as disease vehicles, include air, water, and food. Inanimate agents also include fomites, which are objects on which the pathogen has been deposited. Examples of fomites are toys, clothes, bedding, or surgical instruments. Animate, or living, agents of disease transmission are most often insects, mites, fleas, and rodents. Living agents of transmission are referred to as vectors. Diseases that are spread via indirect contact in hospitals are specifically referred to as nosocomial infections.

Many respiratory viruses and bacterial spores are light enough to be lifted by the wind. These agents can subsequently be inhaled, where they cause lung infections. A particularly important example of an airborne bacterial pathogen is the spore form of the anthrax-causing bacterium *Bacillus anthraci*. This bacterium forms spores that can spread through the air and cause a severe respiratory disease when inhaled. Biological weapons can be equipped with anthrax spores aimed at infecting populations upon detonation. In 2001, the United States was plagued by a bioterrorist who placed spores in mail so that the people who handled the envelopes contracted cutaneous or inhalation anthrax.

A common route of indirect pathogen transmission is via water. The ingestion of contaminated water introduces the microbes into the digestive system, where they can attack the gastrointestinal tract. Some pathogenic organisms use the cells that line the digestive tract in order to gain entry to the bloodstream. From there, an infection can become systemic. A common water borne pathogen is *Vibrio cholerae*, the bacterium that causes cholera. The contamination of drinking water by this bacterium still causes cholera epidemics in some areas of the world.

## Pathogen Transmission

Pathogens are microorganisms such as viruses, bacteria, protozoa, and fungi that cause disease in humans and

Foodborne pathogens are grouped into two categories: those that produce toxins that poison the host and those that infect the host and then grow there. Food poisoning is most often caused by the bacterium *Staphylococcus aureus*, which produces enterotoxins that result in vomiting and diarrhea. The bacterium *Clostridium botulinum* is responsible for the disease botulism, which is an extremely severe and sometimes fatal food poisoning.

Vectors harbor the microorganisms that cause disease and transfer them to humans via a bite or by other contact. *Coxiella burnetti*, the bacterium that causes Q fever, is transmitted to humans from the handling of animals such as sheep. Insects are common vectors of disease. Mosquitos spread the protozoan *Plasmodium vivax* that causes malaria. Deer ticks are responsible for infection by the spirochete *Borrelia burgdorferi* that causes Lyme disease. The bacterium that causes plague *Yersina pestis* is transmitted by the rat flea.

According to the United States Centers for Disease Control, the pathogens that are most likely to be used as biological weapons use a variety of modes of transmission. Included in this list of pathogens are the airborne bacterium *Bacillus anthracis* and the airborne Variola virus that causes smallpox; the foodborne bacterium *Clostridium botulinum*; *Yersina pestis*, which requires a vector; and the Ebola virus, which requires direct bloodborne transmission.

#### ■ FURTHER READING :

##### ELECTRONIC:

United States Centers for Disease Control. "Biological Diseases/Agents." <<http://www.bt.cdc.gov/Agent/agentlist.asp#categorydescriptions>> (February 26, 2003).

##### SEE ALSO

*Anthrax, Terrorist Use as a Biological Weapon*  
*Bioterrorism, Protective Measures*  
*Food Supply, Counter-Terrorism*  
*Infectious Disease, Threats to Security*  
*Vaccines*

## Pathogens

■ BRIAN HOYLE

Pathogens are organisms, frequently microorganisms, or components of these organisms, that cause disease. Microbial pathogens include various species of bacteria, viruses, and protozoa. Many diseases caused by microbial pathogens, and the frequency of these diseases, are a national security issue.

**Pathogens and disease.** A disease is any condition caused by the presence of an invading organism or a toxic component that damages the host. In humans, diseases can be caused by the growth of microorganisms such as bacteria, viruses, and protozoa. Bacterial growth, however, is not mandatory to cause disease. For example, some bacterial pathogens cause disease by virtue of a toxic component of the bacterial cell such as lipopolysaccharide. Finally, the damaging symptoms of a disease can be the result of the attempts by the host's immune system to rid the body of the invader. One example is the immune-related damage caused to the lungs of those afflicted with cystic fibrosis, as the body unsuccessfully attempts to eradicate the chronic infections caused by *Pseudomonas aeruginosa*.

Not all pathogens cause diseases that have the same severity of symptoms. For example, an infection with the influenza virus can cause the short term aches and fever that are hallmarks of the flu, or it can cause more dire symptoms, depending on the type of virus that causes the infection. Bacteria also vary in the damage caused. For example, the ingestion of food contaminated with *Salmonella enteritica* causes intestinal upset. But, consumption of *Escherichia coli* O157:H7 causes a severe disease, which can permanently damage the kidneys and which can even be fatal.

**Types of bacterial pathogens.** There are three categories of bacterial pathogens. Obligate pathogens are those bacteria that must cause disease in order to be transmitted from one host to another. These bacteria must also infect a host in order to survive, in contrast to other bacteria that are capable of survival outside of a host. Examples of obligate bacterial pathogens include *Mycobacterium tuberculosis* and *Treponema pallidum*.

Opportunistic pathogens can be transmitted from one host to another without having to cause disease. However, in a host whose immune system is not functioning properly, the bacteria can cause an infection that leads to a disease. In those cases, the disease can help the bacteria spread to another host. Examples of opportunistic bacterial pathogens include *Vibrio cholerae* and *Pseudomonas aeruginosa*.

Finally, some bacterial pathogens cause disease only accidentally. Indeed, the disease actually limits the spread of the bacteria to another host. Examples of these "accidental" pathogens include *Neisseria meningitidis* and *Bacteroides fragilis*.

**Spread of pathogens.** Pathogens can be spread from person to person in a number of ways. Not all pathogens use all the available routes. For example, the influenza virus is transmitted from person to person through the air, typically via sneezing or coughing. But the virus is not transmitted via water. In contrast, *Escherichia coli* is readily transmitted via water, food, and blood, but is not readily transmitted via air or the bite of an insect.



A worker gets into his chemical protection suit before entering an environmentally sealed tent at Area B-11 on the grounds of Ft. Detrick, Maryland, during a chemical cleanup operation. AP/WIDE WORLD PHOTOS.

While routes of transmission vary for different pathogens, a given pathogen will use a given route of transmission. This has been used in the weaponization of pathogens. The best-known example is anthrax. The bacterium that causes anthrax—*Bacillus anthracis*—can form an environmentally hardy form called a spore. The spore is very small and light. It can float on currents of air and can be breathed into the lungs, where the bacteria resume growth and swiftly cause a serious and often fatal form of anthrax. As demonstrated in the United States in the last few months of 2001, anthrax spores are easily sent through the mail to targets. As well, the powdery spores can be released from an aircraft. Over a major urban center, modeling studies have indicated that the resulting casualties could number in the hundreds of thousands.

Contamination of water by pathogens is another insidious route of disease spread. Water can look crystal clear despite the presence of millions of bacteria in each milliliter. Viruses, which are much smaller, can be present in even higher numbers without affecting the appearance of the liquid. Thus, water can be easily laced with enough pathogens to cause illness.

Food-borne pathogens cause millions of cases of disease and hundreds of deaths each year in the United

States alone. Frequently the responsible microbes are bacteria, viruses, or protozoa that usually reside in the intestinal tract of humans or other creatures. Examples of such microorganisms include *Escherichia coli* O157:H7, *Campylobacter jejuni*, and rotavirus.

Pathogens can be transmitted to humans through contact with animals, birds, and other living creatures that naturally harbor the microorganism. The agent of anthrax—*Bacillus anthracis*—naturally dwells in sheep. Other examples include *Brucella abortus* (Brucellosis), *Coxiella burnetii* (Q fever), and viruses that cause hemorrhagic fevers such as Ebola and Marburg.

**Pathogenic mechanisms.** Microorganisms have various strategies to establish an infection in a host. Some microorganisms recognize molecules on the surface of the host cell, and use these as receptors. The binding of bacteria or viruses to receptors brings the microorganism in close contact with the host surface.

The nature of the interaction between the host receptor molecule and the attachment molecule on the surface of the bacteria, virus, or protozoan has in some cases been defined, even to the genetic level. The use of recombinant



DNA technology—where a target section of genetic material is removed from one organism and inserted into a certain region of the genetic material of another organism, in a way that does not affect the expression of the gene—allows the genetic manipulation of a microorganism so as to enhance its ability to cause an infection. Alternatively, inserting a gene that codes for a toxin into a bacterium that is a normal inhabitant of an environment like the intestinal tract could produce a formidable pathogen. This altered bacteria would readily associate with host cells, but would also carry the toxin.

Viruses almost always damage the host cells. Because viruses cannot reproduce on their own, they rely on the replication mechanism of the host cell to make more copies of themselves (i.e., they are obligate pathogens). Then, the new viral particles will exit the cell and search for another cell to infect. This exit is often very physically damaging to the host cell. Thus, viral infections can be detrimental because of the loss of function of host cells.

Some viral pathogens are capable of causing a disease long after they have infected a host. This delayed response occurs because the viral genetic material becomes incorporated into the genetic material of the host. Thereafter, the viral genetic material is replicated along with that of the host, using the replication enzymes and other machinery of the host. But, in response to a number of signals, the viral material can be excised from the host material and form the template for the manufacture and assembly of new virus particles. A prominent example of such a virus is the Human Immunodeficiency Virus, which is acknowledged to be the cause of Acquired Immunodeficiency Syndrome.

Because viruses must infect other cells in order to replicate, they have developed means of escaping (at least for a time) the defensive responses of the host. This efficiency of attack has not escaped the attention of molecular biologists bent on the malicious use of viruses. By inserting gene coding for a toxic compound into a viral genome, particularly into the genome of an infectious virus (i.e., influenza or cold viruses) the virus becomes a bioweapon. For example, scientists in the former Soviet Union attempted to construct an influenza virus that contained the gene coding for cobra toxin.

#### ■ FURTHER READING :

##### BOOKS:

- Fields, Bernard N., Peter M. Howley, and Diane E. Griffin, eds. *Virology*. Philadelphia: Lippincott Williams & Wilkins, 2001.
- Shnayerson, Michael, and Mark J. Plotkin. *The Killers Within: The Deadly Rise of Drug Resistant Bacteria*. New York: Little Brown & Company, 2002.
- Smith, H., C. J. Dornan, G. Dougan, et al., eds. *The Activities of Bacterial Pathogens In Vivo*. River Edge, NJ: World Scientific, 2001.

##### ELECTRONIC:

Centers for Disease Control and Prevention. "Disease Information." Special Pathogens Branch. July 26, 2002. <<http://www.cdc.gov/ncidod/dvrd/spb/mnpages/disinfo.htm>> (28 December 2002).

##### SEE ALSO

*Biocontainment Laboratories*  
*Decontamination Methods*  
*Infectious Disease, Threats to Security*

---

## Patriot Act Terrorist Exclusion List

---

As mandated by the Patriot Act of 2001 (officially the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act), the United States Department of State Office of the Coordinator for Counterterrorism, in conjunction with the Attorney General, compiles a Terrorist Exclusion List (TEL) of groups and individuals excluded entry into the United States because of terrorist related activities. Individuals and organizations who commit, incite, or aid in the commission of a terrorist act with the intention to cause death or bodily injury may be placed on the TEL. Acts prior to the commission of a terrorist act, or that aid terrorist organizations also qualify individuals and groups for exclusion. Such preparation or aid can include—but is not limited to—the gathering of intelligence for, or financial support of, terrorist activities.

For purpose of compiling the TEL, the Department of State use the definition of terrorism set forth in United States law and that specifically defines terrorism as "the commission of acts, formulation of plans, or threat to engage in unlawful acts that include—but are not limited to—hijacking, sabotage, the taking of hostages, a violent and deliberate attack on civilians; assassination; the use or transportation of nuclear, chemical, or biological weapons."

TEL designation is intended to disregard supposed political or ideological purposes for terrorist acts while providing a legal framework to exclude or deport aliens associated with TEL-designated organizations. TEL designations are also intended to deter contributions to terrorist groups, to increase public awareness of such groups, and isolate designated organizations.

#### ■ FURTHER READING :

##### ELECTRONIC:

U.S. Department of State. International Information Programs. Fact Sheet: Terrorist Exclusion List Bolsters Homeland Security. November 15, 2002. <<http://usinfo.state.gov/topical/pol/terror/02111803.htm>> (April 16, 2003).

## SEE ALSO

*Coordinator for Counterterrorism, United States Office  
Terrorist and Para-State Organizations  
Terrorist Organization List, United States  
Terrorist Organizations, Freezing of Assets  
Terrorist Threat Integration Center*

---

## Patriot Act, United States

---

The Patriot Act, or Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, was signed into law on October 26, 2001, in the wake of terrorist attacks on the World Trade Center and Pentagon. The legislation grants law enforcement and intelligence agencies more power to detain and question suspects for longer periods of time, and increases their ability to conduct surveillance operations.

The act further calls on federal agencies to share information regarding terrorist activities with each other, and with foreign intelligence services if necessary. Thus, domestic law enforcement was granted new privileges to deal directly with international agencies. The bill asks, but cannot compel that foreign intelligence services reciprocate and share information with United States authorities.

Some provisions, such as the authority to intercept wire communications that possibly relate to terrorism and the sharing of criminal investigative information, are set to expire in 2005. Some debated provisions, however, will remain indefinitely. The sharing of grand jury information and the ability to search without a warrant in limited cases, for example, do not expire.

The Patriot Act extended the government's surveillance authority under the Foreign Intelligence Surveillance Act (FISA), which was passed by the United States Congress in 1978. New powers included roving wiretap authority (the surveillance of communications related to an individual or organization without regard to particular telephone line, computer station, or other mode of communication to be monitored). Other extensions included a more liberalized use of pen register, trap and trace devices (removing the need to assert that the surveillance target is "an agent of a foreign power"). In May 2002, the Foreign Intelligence Surveillance Court specifically rejected Justice Department attempts at "information screening" and "minimization" procedures intended to allow the use of material gathered under Foreign Intelligence Surveillance Court authorization in criminal proceedings. The Department of Justice appealed the ruling to the Foreign Intelligence Surveillance Court of Review.

Supporters of the Patriot Act say that the legislation is not drastic and that law enforcement and intelligence

must not be hampered in their pursuit of suspected terrorists. Opponents assert the law infringes on constitutional protections on legal search, seizure, and detention of property and persons. Some are wary of the implications of the Patriot Act on Internet and computer privacy. Others argue that the measure is acceptable during wartime, or when specifically applied against suspected terrorists, but that broad interpretation and application of the law could be problematic in its constitutionality.

The newness of the law means that it has yet to be both fully implemented and ultimately tested. Thus, a final assessment on its efficacy, intent, application, and legacy will require the perspective of time.

## SEE ALSO

*Homeland Security, United States Department of  
September 11 Terrorist Attacks on the United States*

---

## Patriot Missile System

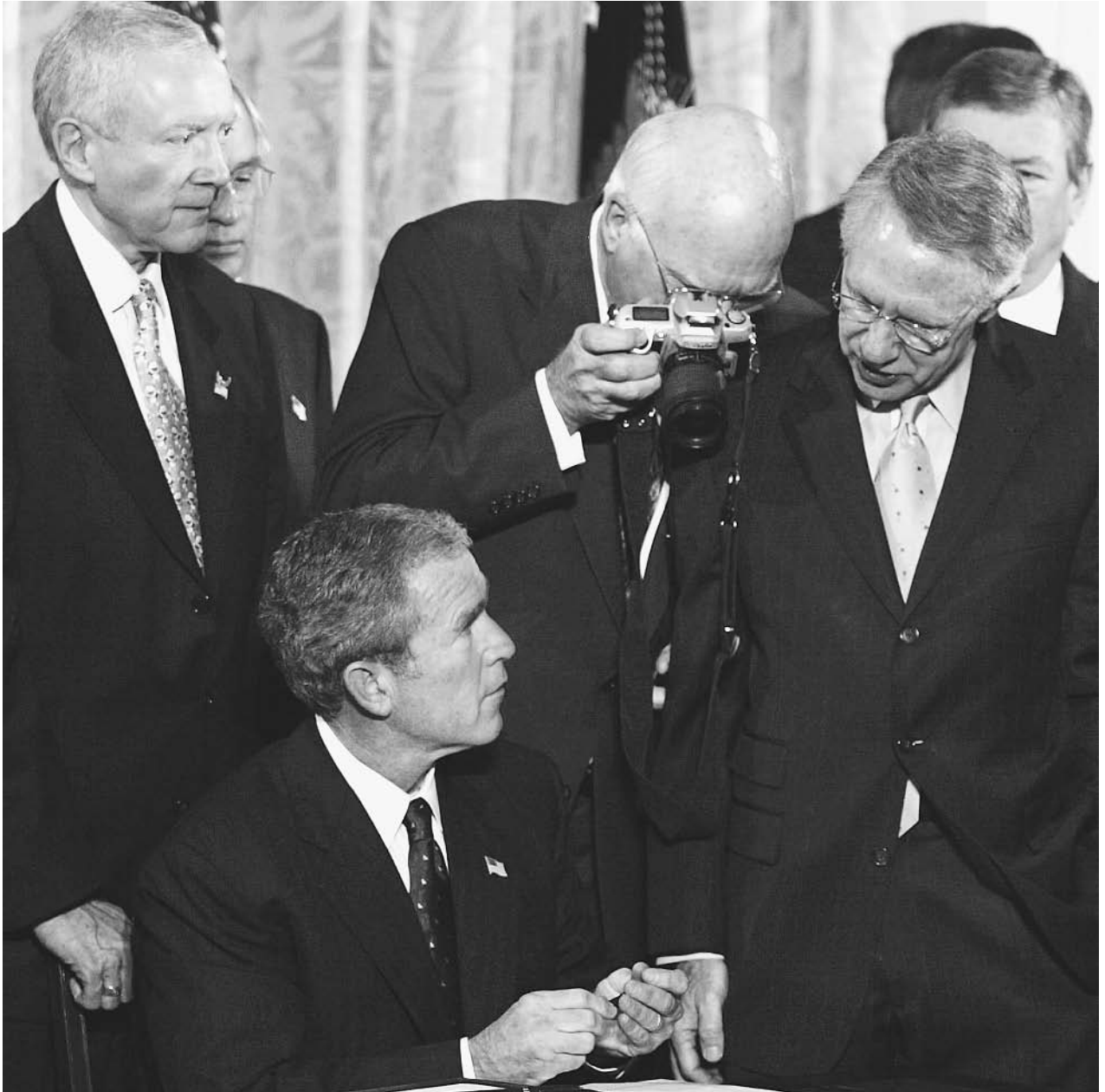
---

Among the world's most advanced ground-based air defense systems, the Patriot Air and Missile Defense System is in service to the United States and other nations. The missile system, produced jointly by Raytheon and Lockheed Martin Missiles and Fire Control, was a notable feature in the Persian Gulf War of 1991 and Operation Iraqi Freedom in 2003. Since 1991, the U.S. Department of Defense (DOD) has spent more than \$3 billion in further improvements. As effective as the Patriot has been, however, its record is not flawless.

Among the most significant aspects of the Patriot missile system are the multifunction phased array radar, the track-via-missile guidance with midcourse correction commands and ground radar downlink, and the human override to its automated operations. The system also includes an engagement control station, electronic power plant vehicle, as many as 16 remote launching stations (each with four Patriots ready to fire), and an antenna mast group for communications.

In the Persian Gulf War, allied forces used the Patriot to stop Iraqi Scud missiles, particularly when Saddam Hussein's military fired on Israel. After the war ended, DOD invested in numerous upgrades such as the development of the Patriot Guidance Enhanced Missile Plus (GEM+), which includes a new fuse and a low-noise front end that increases the sensitivity to low radar targets. With 148 missiles contracted, Raytheon delivered the first GEM+ models in November 2002.

Despite the successes of the Patriot in Operation Desert Storm, there were mishaps, as when a Patriot at Dharan, Saudi Arabia, failed to intercept an incoming Scud on February 25, 1991, resulting in the deaths of 28 Americans. During Operation Iraqi Freedom 12 years later, the Patriot was involved in several unfortunate incidents, including the downing of a British Royal Air Force Tornado



Senator Patrick Leahy (with camera) peers over the shoulder of President Bush during a ceremony for the signing of the Patriot Act in the White House East Room in October 2001. AP/WIDE WORLD PHOTOS.

with two airmen aboard on March 23, 2003. Aside from the United States, nations that possess Patriots include Germany, Japan, Israel, Saudi Arabia, Kuwait, Taiwan, Greece, and the Netherlands. Patriots have also been cleared for sale to Egypt.

#### ■ FURTHER READING:

##### PERIODICALS:

Kilian, Michael. "Patriot Missile Miscalculations a Cause for U.S. Concern." *Chicago Tribune*. (March 27, 2003): 5.

Marshall, Eliot. "Patriot's Scud Busting Record Is Challenged." *Science* 252, no. 5006 (May 3, 1991): 640–641.

##### ELECTRONIC:

GAO Report: Patriot Missile Defense. Federation of American Scientists. <<http://www.fas.org/spp/starwars/gao/im92026.htm>> (April 7, 2003).

Patriot Missile Air Defense System, USA. Army Technology. <<http://www.army-technology.com/projects/patriot/>> (April 7, 2003).



A Patriot anti-missile missile is launched during a 2001 joint Israeli-American military exercise in the Negev Desert in southern Israel. AP/WIDE WORLD PHOTOS.

SEE ALSO

- Ballistic Missile Defense Organization, United States*
- Ballistic Missiles*
- Cruise Missile*
- IFF (Identification Friend or Foe)*
- Iraqi Freedom, Operation (2003 War Against Iraq)*
- Persian Gulf War*
- Strategic Defense Initiative and National Missile Defense*

destroyers, and eight battleships along “Battleship Row” were severely damaged, and two battleships, the *Okla-homa* and the *Arizona*, were sunk. Additionally, nearly 350 American warplanes on Oahu were destroyed, virtually all that were on the ground. Over 2,400 U.S. servicemen lost their lives, and nearly 1,200 were wounded. The success of the daring attack severely impaired America’s ability to check the expansion of the Japanese empire in the Pacific during the first years of WWII.

## Pearl Harbor, Japanese Attack on

■ MICHAEL J. O’NEAL

On December 7, 1941, Japanese military forces attacked the United States naval fleet anchored at Pearl Harbor on the Hawaiian island of Oahu. The surprise attack nearly devastated the American Pacific fleet. Three cruisers, three

**Background.** As an island nation, Japan had developed a rich and complex social structure. It resisted westernization by sealing itself off from contact with the outside world, particularly Europe and the United States. By the early twentieth century, though, Japan’s efforts to achieve self-sufficiency were failing, for the nation lacked its own raw materials and other resources. Some members of the ruling class argued that Japan could grow and prosper only by modernizing and adopting Western technology. Japanese nationalists, though, advocated a different path: the establishment of an empire that would not only elevate Japan’s stature in the eyes of the world but also



Three U.S. battleships are hit from the air during the Japanese attack on Pearl Harbor on December 7, 1941. From left are: USS *West Virginia*, severely damaged; USS *Tennessee*, damaged; and USS *Arizona*, sunk. AP/WIDE WORLD PHOTOS.

guarantee access to the resources the nation needed. Moreover, many members of the nation's traditional warrior class—the Samurai—were embittered by the aftermath of World War I. Japan had backed the victorious Allies, but the Samurai believed that in the peace negotiations following the war the United States and Great Britain had treated Japan as a second-class nation. They, too, longed to assert Japan's place in world affairs.

Japan began to flex its muscles in 1931. Japanese forces stationed in Manchuria, northeast of China, to protect a Japanese railway that transported goods and raw materials out of the country suddenly seized control of all of Manchuria. Then in 1937, Japanese forces attacked the eastern provinces of China, seizing China's capital, Nanking, and the old capital, Beijing, in brutal fashion. Observers in the West were horrified by reports of the atrocities against civilians committed by Japanese invaders in the so-called "Rape of Nanking." Under the leadership of Minister of War Hideki Tojo, Japan's objective was to establish a

defensive perimeter—the "Greater East Asia Co-Prosperty Sphere"—in the western Pacific. This perimeter was to extend from the Jurile Islands northeast of Japan, south to the Marianas and Marshall Islands, west through the Solomon Islands, New Guinea, and the East Indies, then northward into the Indian Ocean and southeast Asia. Tojo believed that Japan could thus drive out the Western powers, achieve a position of preeminence in East Asia, and free the nation from its dependence on Western oil, coal, rubber, ore, and other vital resources.

Tojo's strategy, however, was bringing him ever closer to conflict with those powers. The Dutch, for example, controlled the East Indies, France had a presence in Indo-China, the United States controlled the Philippines, and Malaya was a British colony. Concerned about Japanese aggression, Holland, Great Britain, and the United States imposed a trade embargo on Japan on July 26, 1941,

cutting off supplies of resources to the increasingly belligerent nation. Tojo, now prime minister, was convinced that the West's goal was to starve Japan into submission.

Events came to a boil in September, 1941. United States Secretary of State Cordell Hull demanded that Japan withdraw its troops from China and Southeast Asia. While many Japanese military leaders quailed at the prospect of going to war with the United States, Tojo convinced them that acceding to American demands would be a humiliating diplomatic defeat. While carrying on protracted—and deceptive—negotiations with the United States, Japan invaded Thailand, Malaya, Burma, and the East Indies. And on November 26, the Japanese navy set sail for Pearl Harbor, where most of the U.S. Pacific fleet was docked.

**The attack.** Traveling under strict radio silence and screened from view by a large weather front, the Japanese battle fleet—six aircraft carriers, two battleships, two cruisers, and nine destroyers—remained undetected until it came within two hundred miles of the Hawaiian Islands. On the morning of December 7, 183 torpedo bombers and dive-bombers took off from the aircraft carriers. The Japanese pilots knew exactly where they were going because spies on the islands had given them elaborate and detailed scale models of the base, including Battleship Row. Because it was Sunday morning, most of the U.S. naval personnel were ashore, and most of the anti-aircraft defenses were unmanned. At 7:49 AM local time, the attack began—and by 8:12, much of the fleet had been damaged or sunk. A second wave of bombers arrived at nine o'clock to finish what the first wave had started. In a little more than an hour, the United States fleet was severely crippled. Two days later, on December 9, the United States declared war on Japan.

**Japanese espionage.** The U.S. Army's Hawaii Department was charged with coastal defenses on the islands in 1941. In a 1955 interview, its chief, Major General Charles D. Herron, stated, "It was a matter of common knowledge that the Japanese Consulate in Honolulu was the hotbed of espionage in Oahu." In large part, the attack on Pearl Harbor was so successful because Japanese spies, under cover of "diplomatic" posts, were able to blend easily with the large Japanese population on the islands and in the process gather valuable intelligence.

One such diplomat, for example, was Takeo Yoshikawa, who openly arrived in Hawaii by ship on March 27, 1941, as Tadashi Morimura. Yoshikawa was a trained spy assigned to the Japanese consulate on Oahu. He took a second-story room that gave him a view of Pearl Harbor and Hickam Field, where the American air fleet was based. In the weeks and months after his arrival, Yoshikawa moved freely about the island. At times he would loiter in a sugar cane field near Pearl Harbor, posing as a fieldworker. At other times he would observe Pearl Harbor from a peninsula at the end of the island or through telescopes

for sightseers at a Japanese-owned restaurant on a hill overlooking the harbor. Little about his work was glamorous. He made notes, took photos, chartered small boats and planes. He even mailed back home postcards with aerial views of Pearl Harbor that helped planners construct mock-ups used to train bomber pilots for the raid. In these endeavors, he was ably supported not only by his superiors in the consular office but even by the taxi driver who frequently drove him around the island. He observed, for example, that there tended to be a large number of ships in port on Saturdays and Sundays, fewer on weekdays. He also observed American air patrols, noticing that they tended rarely to fly to the north. The kinds of details Yoshikawa meticulously noted and passed along to military planners in Japan proved invaluable on December 7, a Sunday, when Japanese planes approached Oahu from the north.

**American intelligence.** A question that continues to intrigue historians is how American intelligence could have failed so spectacularly, given the circumstances. The diplomatic situation was tense, and growing tenser. It was known that Germany, a Japanese ally, was pressing Japan to take action to divert American attention away from Europe. As early as January 27, 1941 Joseph Grew, the U.S. ambassador in Japan, reported to Secretary of State Hull that the embassy had learned from Japanese sources that a mass attack on Pearl Harbor was planned in case hostilities broke out. The United States had broken the Japanese diplomatic code (called Purple), so war planners from the president on down knew that spies had been reporting on the fleet deployment in Hawaii. In the weeks and days before the attack, encrypted diplomatic traffic became heavier, and increasingly ominous. On November 19, for example, American codebreakers intercepted a message from Tokyo to diplomatic posts in Washington, D.C., and several West Coast cities. The message instructed these offices to destroy all codes, coding machines, papers, and the like if they heard the words "East Wind Rain" (*Higashi No Kazeame*) in the daily weather forecast. On Thursday, December 4, the United States intercepted the so-called "winds message." Even on the morning of December 7, Army Chief of Staff General George C. Marshall sent an urgent warning to commanders in the Pacific that intercepted Japanese diplomatic messages strongly suggested an attack was imminent. Military signalmen, however, could not raise Pearl Harbor on military channels, so the message was sent by slower commercial cable. By the time it arrived, Japanese planes were in the air over Pearl Harbor.

Given this flood of intelligence, historians and military analysts question why the military failed to take steps to defend Pearl Harbor. One answer might lie in the flood of messages intercepted. Few of the hundreds of intercepted diplomatic messages specifically mentioned Pearl Harbor. Those that did—requests for information on fleet deployment at Pearl, for example—were part of general

requests for similar information about numerous American bases in the Pacific. While events proved that Pearl Harbor was Japan's intended target, that seemed less apparent in 1941, when bits of unconnected intelligence arrived on the president's desk on a daily basis and no one was charged with the responsibility of "connecting the dots." Ironically, the only American official who had clear intelligence regarding Pearl Harbor was FBI director J. Edgar Hoover. The information, though, was provided by a Yugoslav double agent named Dusko Popov, who had received clear indications of Japanese intentions while operating in Germany. Hoover, though, hated Slavs, despised Popov, cut his interview with Popov short, and failed to send Popov's vital information on to the president.

Although evidence is lacking or conflicting, some revisionist historians have presented scenarios that may explain U.S. failures to protect the fleet. Some of these scenarios involve a deliberate disregard for intelligence by U.S. and British leaders on the grounds that the attack would likely force America's entrance into WWII. Most historians, however, dismiss these theories as either inconsistent with the greater body of evidence, or simply convoluted and needlessly complex explanations of normal intelligence and communications failures.

#### ■ FURTHER READING :

##### BOOKS:

- Andrew, Christopher. *For the President's Eyes Only: Secret Intelligence and the American Presidency from Washington to Bush*. New York: HarperCollins, 1995.
- Benson, Robert Louis. *A History of U.S. Communications Intelligence During World War II: Policy and Administration*. Washington, D.C.: Center for Cryptologic History, National Security Agency, 1997.
- Persico, Joseph E. *Roosevelt's Secret War: FDR and World War II Espionage*. New York: Random House, 2001.
- Prange, Gordon W. *At Dawn We Slept: The Untold Story of Pearl Harbor*. New York: McGraw-Hill, 1981.
- Winton, John. *Ultra in the Pacific: How Breaking Japanese Codes & Cyphers Affected Naval Operations Against Japan: 1941-45*. London: Leo Cooper, 1993.

##### ELECTRONIC:

- Singh, Simon. "US Codebreakers in World War II." <<http://www.vectorsite.net/ttcode7.html>> (January 9, 2003).

##### SEE ALSO

*Cipher Machines*  
*Codes and Ciphers*  
*Cryptology, History*  
*Double Agents*  
*Purple Machine*  
*World War II*

## PEN Register.

SEE *Internet Surveillance*.

## Pentagon Terrorist Attack.

SEE *September 11 Terrorist Attacks on the United States*.

## People Against Gangsterism and Drugs (PAGAD)

People Against Gangsterism and Drugs (PAGAD) was formed in 1996 as a community anti-crime group fighting drugs and violence in the Cape Flats section of Cape Town, South Africa, but by early 1998 it had also become anti-government and anti-Western. PAGAD and its Islamic ally Qibla view the South African Government as a threat to Islamic values and consequently, promote a greater political voice for South African Muslims. Abdus Salaam Ebrahim currently leads both groups. PAGAD's G-Force (Gun Force) operates in small cells and is believed to be responsible for carrying out acts of terrorism. PAGAD uses several front names, including Muslims Against Global Oppression (MAGO) and Muslims Against Illegitimate Leaders (MAIL), when launching anti-Western protests and campaigns. PAGAD's activities were severely curtailed in 2001 by law enforcement and prosecutorial efforts against leading members of the organization. PAGAD's bombing targets have included South African authorities, moderate Muslims, synagogues, gay nightclubs, tourist attractions, and Western-associated restaurants. PAGAD is believed to have masterminded the bombing in August, 1998, of the Cape Town Planet Hollywood.

Estimated at several hundred members, PAGAD's G-Force probably contains fewer than 50 members. PAGAD operates mainly in the Cape Town area, South Africa's foremost tourist venue.

#### ■ FURTHER READING :

##### ELECTRONIC:

- CDI (Center for Defense Information), Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <<http://www.cdi.org/terrorism/terrorist.cfm>> (April 17, 2003).
- Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).
- Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001." Annual Report: On the Record Briefing. May 21, 2002. <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).
- U.S. Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

## SEE ALSO

*Terrorism, Philosophical and Ideological Origins  
Terrorist and Para-State Organizations  
Terrorist Organization List, United States  
Terrorist Organizations, Freezing of Assets*

## Persian Gulf War

### ■ JUDSON KNIGHT

The Persian Gulf War, in which a coalition led by the United States drove Iraqi forces out of Kuwait in early 1991, was one of the most successful campaigns in history. At a cost of less than 300 Allied lives, coalition troops, whose military actions were largely funded by Saudi Arabia, drove out Saddam Hussein's forces. Thousands of Iraqi lives were lost in the process, however. In their victory, the coalition depended in large part on advances in military technology by the United States, whose arsenal included tools ranging from the F-117A stealth fighter to the M1A1 Abrams tank, and from the Global Positioning System (GPS) to unmanned drones and Patriot missiles. Less clearly successful was U.S. intelligence, which had failed to predict the war. Equally questionable was the ultimate outcome of the war, whose scores would not fully be settled until 12 years later.

The Persian Gulf War is sometimes called simply the Gulf War or Operation Desert Storm, after the U.S.-led campaign that comprised the bulk of the fighting. It may ultimately come to be known as "Gulf War II," or "Persian Gulf War II," with the 2003 operation in Iraq becoming the third in this series. The first, also known as the Iran-Iraq War, lasted from 1980 to 1988, and pitted the dictatorship of Saddam Hussein against the Islamic theocracy in Iran.

Both regimes had taken power in 1979, but the conflict concerned long standing disputes involving lands on the borders between the two nations. In the ensuing hostilities, most nations—including much of the Arab world, the United States, western Europe, and the Soviet bloc—supported Iraq, generally regarded as the lesser of two evils. (Both the Americans and the Soviets also gave covert support to the Iranians as well.) The war, which cost some 850,000 lives, resulted in a stalemate, and both nations built monuments to their alleged victories.

In the aftermath of the first Gulf War, analysts working for the U.S. Central Intelligence Agency (CIA) prepared a report on the likelihood of Iraqi aggression in the near future. According to the now-infamous study, Saddam had so overextended his resources in the war with Iran that he would not take any major aggressive action for at least three years. In this instance, the CIA underestimated Saddam's penchant for military adventurism.

## Invasion and Buildup

On August 2, 1990, without advance warning, Iraqi tanks and troops rolled into neighboring Kuwait. Both nations possessed considerable oil wealth, but Kuwait was by far the richer of the two, and Iraq—particularly under Saddam's regime—had long had designs on Kuwait. Given the importance of oil from the Persian Gulf region, which at that time fueled a great part of the world, neither the United States nor the United Nations (UN) Security Council was inclined to ignore Hussien's aggressive action.

The Security Council on August 3 called for an Iraqi withdrawal, and on August 6 it imposed a worldwide ban on trade with Iraq. On August 5, President George H. W. Bush declared that the invasion "will not stand," and a day later, King Fahd of Saudi Arabia met with U.S. Defense Secretary Richard Cheney to request military assistance. Saudi Arabia, Japan, and other wealthy allies would underwrite most of the \$60 billion associated with the resulting military effort. By August 8, U.S. Air Force fighters were in Saudi Arabia.

Numerous countries were involved in the military buildup during late 1990, a program known as Operation Desert Shield. By January 1991, the United States alone had some 540,000 troops, along with another 160,000 from the United Kingdom, France, Egypt, Saudi Arabia, Syria, Kuwait, and other nations. On November 29, 1990, the Security Council authorized use of force against Iraq unless it withdrew its troops by January 15. Saddam's only response was to continue building his troop strength in Kuwait, such that by the time the Allies counterattacked, he had some 300,000 men on the ground.

On January 17, 1991, Operation Desert Shield became Operation Desert Storm, which consisted largely of bombing campaigns against Iraq's command and control, infrastructure, and military assets. In retaliation, Iraq attacked Israel with Scud missiles on January 18. A great portion of the Allied losses occurred in this initial phase, when the Iraqis shot down several low-flying U.S. and British planes.

After thus severing the tail of the invading force, the Allies in February began concentrating on Iraqi positions in Kuwait. Having initially planned an amphibious landing, Allied commander General H. Norman Schwarzkopf instead opted for an armored assault. On February 24, in a campaign phase named Operation Desert Sabre, Allied troops moved northward from Saudi Arabia and into Kuwait. By February 27, they had taken Kuwait City.

At the same time, operations in Iraq itself continued. In the only major bombing run on the capital city of Baghdad, Stealth fighters struck Iraqi intelligence headquarters, while U.S. Army Special Forces teams inserted themselves deep in Iraq. In the southern part of the country, U.S. tanks pounded Iraqi armored reserve forces, while Allied ground forces neutralized Hussien's "elite"





A line of captured Iraqi soldiers are marched through the desert in Kuwait past a group of U.S. Marine vehicles during the 1991 Persian Gulf War. AP/WIDE WORLD PHOTOS.

Republican Guard south of Basra. President Bush declared a cease-fire on February 28.

The war had lasted 42 days, and the principal campaign, the mid-January bombing, took just over 100 hours. Credit for this extraordinary success goes to a number of factors, not least of which was strong leadership. On the military side, there was Schwarzkopf on the ground, and in Washington, General Colin Powell, Chairman of the Joint Chiefs of Staff, who served as the principal military spokesman during the war. In this, the first major U.S. action since the end of fighting in Vietnam nearly two decades earlier, the performance of both leaders and troops showed that military capabilities had improved extraordinarily since then.

Among the civilian leaders were Cheney, Secretary of State James Baker, National Security Advisor Brent Scowcroft, and President Bush. The president, sometimes criticized for a failure to communicate his aims to his subordinates or the public as a whole, was quite clear in his objectives for the Persian Gulf War. On January 15, 1991, Bush sent his principal security advisors a memorandum which outlined four major aims: to force an Iraqi withdrawal from Kuwait, to restore Kuwait's government, to protect American lives, and to promote stability and security in the Gulf region.

Another factor in the success—and another point of comparison with Vietnam—was the near-unanimous support for the action. Whereas American allies and foes alike questioned the value of the action in Vietnam, virtually no one other than Saddam's regime (along with a handful of antiwar protestors at home) opposed the U.S. effort to liberate an invaded nation. This support was helped rather than hurt by an unprecedented level of television coverage. While Vietnam became known as "the first televised war," TV reporting in the 1960s and 1970s was minimal compared to the round-the-clock reportage offered by cable outlets, most notably the Cable News Network (CNN), in 1990 and 1991.

**The U.S. arsenal.** While human factors deserve a great deal of credit for the success of Allied operations in the Persian Gulf War, the war would not have been won as efficiently without the technological superiority offered by modern weaponry. Among the tools in the U.S. arsenal were a variety of aircraft, including the AH-64 Apache helicopter, the leading anti-armor attack chopper. Introduced in 1984, the Apache could operate in conditions of darkness or low visibility, and was made to sustain heavy pounding from anti-aircraft guns.

The E-3 Sentry AWACS (airborne warning and control system) was a masterpiece of modern technology. Packed with electronics, the aircraft—based on the Boeing 707 and introduced in 1977—was made to identify enemy aircraft, jam enemy radar, guide bombers to their targets, and manage the flow of friendly aircraft. Even more cutting-edge were the Pointer and Pioneer drones, or remotely piloted vehicles (RPVs).

Based on Israeli designs and first used by the United States during the war, the RPVs served as airborne spy platforms. The Pioneer, with a range of about 100 miles (161km) and a flight duration of five hours, could take high-definition pictures from 2,000 feet (610 meters) and transmit them to a processing center. In addition to its video cameras, it was equipped with infrared heat sensors, and provided a wealth of intelligence on everything from enemy troop movements to the recommended path for Tomahawk cruise missiles.

Other aircraft included the B-52 Stratofortress bomber, the F-117A Stealth fighter, and the E-8G JSTARS surveillance aircraft. Among the other notable weapons used in the Persian Gulf War were the M1A1 Abrams tank, the Bradley Fighting Vehicle, the MIM-104 Patriot missile defense system, and the Tomahawk cruise missile. High above the ground was the GPS, whose 24 satellites helped soldiers find their bearings in the desert, and assisted artillery in targeting.

**Controversies.** More controversial than the role of weapons systems was that of intelligence in the Persian Gulf War. The CIA did not inspire a great deal of confidence, either with its initial estimate of Iraqi intentions or from its August 1996 “Final Report on Intelligence Related to Gulf War Illnesses.” In the wake of illnesses that broke out among returning personnel, the CIA sought to investigate the connection between these conditions and Iraqi use of chemical or biological agents. The CIA report found no evidence that Iraq had intentionally used such weapons against the United States, even though Saddam used chemical weapons against rebellious Kurds in the north.

More successful was the performance of Defense Department intelligence and related activities, both on the part of the Defense Intelligence Agency (DIA) and various military intelligence and psychological warfare units. DIA began operations in Iraq long before the war, and regularly gathered intelligence reports that proved invaluable to military leadership. The same was true of military intelligence units, while psychological operations had an immeasurable impact by coercing Iraqis to provide the Allies with intelligence on their forces’ activities and capabilities.

In addition to controversies over the success of intelligence, there remained questions concerning the success of the war as a whole. This fact was symbolized by the failure of Bush—who, after the war, had the highest poll numbers of any U.S. President since scientific polling began—to gain reelection in 1992. Ironically, Saddam

Hussein, who many U.S. leaders had expected to be toppled in the unrest that followed the war, remained in power despite UN sanctions and the imposition of a no-fly zone over the northern and southern portions of the country. Among the factors cited for Bush’s sudden loss of popularity from mid-1991 onward (in addition to an economic slowdown and clever campaigning by challenger William J. Clinton) was his failure to remove Saddam Hussein. However, as Bush rightly noted, such action was not within his mandate from the UN.

In 1993, the CIA uncovered evidence that Saddam Hussein had attempted to assassinate Bush, in response for which U.S. warships fired 23 cruise missiles at Iraqi secret service headquarters. The years that followed saw a lengthy process of UN and U.S. attempts to find weapons of mass destruction thought to be hidden in Iraq continually thwarted by Saddam Hussein. When he evicted UN inspectors in 1998, the United States and United Kingdom launched a four-day bombing campaign, Desert Fox, against Iraq.

Although overt evidence was lacking, some in the U.S. intelligence and defense communities suspected Iraqi ties to the 1993 World Trade Center bombing, and after the 2001 destruction of those buildings, President George W. Bush indicated that the attacks had been sponsored or at least abetted by Iraq. In March, 2003, the United States launched Operation Iraqi Freedom, a land invasion of Iraq. Though many putative experts claimed that the campaign would not be as successful as the Persian Gulf War, this one—while much less popular globally—was actually shorter, and achieved something the earlier war did not: the removal of Saddam Hussein from his position of leadership. Assisting the younger Bush were several figures from the Persian Gulf War, including Cheney and Powell, now vice president and secretary of state respectively.

#### ■ FURTHER READING:

##### BOOKS:

- Allen, Thomas B., F. Clinton Berry, and Norman Polmar. *War in the Gulf*. Kansas City, MO: Andrews & McMeel, 1991.
- Atkinson, Rick. *Crusade: The Untold Story of the Persian Gulf War*. Boston: Houghton Mifflin, 1993.
- Clancy, Tom, and Fred Franks. *Into the Storm: A Study of Command*. New York: Putnam, 1997.
- Dunnigan, James F., and Austin Bay. *From Shield to Storm: High-Tech Weapons, Military Strategy, and Coalition Warfare in the Persian Gulf*. New York: W. Morrow, 1992.
- Freedman, Lawrence, and Efraim Karsh. *The Gulf Conflict, 1990–1991: Diplomacy and War in the New World Order*. Princeton, NJ: Princeton University Press, 1993.
- Gordon, Michael R., and Bernard E. Trainor. *The Generals’ War: The Inside Story of the Conflict in the Gulf*. Boston: Little, Brown, 1995.

Hawley, T. M. *Against the Fires of Hell: The Environmental Disaster of the Gulf War*. New York: Harcourt Brace Jovanovich, 1992.

MacArthur, John R. *Second Front: Censorship and Propaganda in the Gulf War*. New York: Hill and Wang, 1992.

#### ELECTRONIC:

Fog of War. WashingtonPost.com. <<http://www.washingtonpost.com/wp-svr/inatl/longterm/fogofwar/fogofwar.htm>> (April 13, 2003).

Frontline: The Gulf War. Public Broadcasting System. <<http://www.pbs.org/wgbh/pages/frontline/gulf/>> (April 13, 2003).

#### SEE ALSO

*B-52*

*Bush Administration (1989–1993), United States National Security Policy*

*Cruise Missile*

*F-117A Stealth Fighter*

*GPS*

*Information Warfare*

*Iraqi Freedom, Operation (2003 War Against Iraq)*

*Iraq, Intelligence and Security Agencies*

*Iraq War: Prelude to War (The International Debate Over the Use and Effectiveness of Weapons Inspections.)*

*J-Stars*

*Kuwait Oil Fires, Persian Gulf War*

*Patriot Missile System*

abuses. Restructuring in 2002 sought to minimize the organization's ties to political espionage during the Fujimori regime.

Peru's Technical Police (PT) is the primary communications and electronic surveillance force. The agency works closely with the other organizations in the Peruvian intelligence community, but has been accused on several occasions of aiding government-backed political espionage against dissidents.

Peru's military intelligence community is organized within the nation's army and administered by Army Intelligence Directorate (DINTE). The Army Intelligence Service (SIE) focuses on foreign intelligence and the protection of military installations. In addition, individual military units in the Peruvian navy and air force may maintain their own strategic intelligence forces.

The prevalence of drug trafficking networks in the region, as well as a rise in paramilitary organizations connected to organized crime, prompted the development of the National Counter-terrorism Division, or Dincote, as it is more commonly known. Dincote specializes in anti-terrorism intelligence, using both electronic surveillance and human intelligence to infiltrate anti-government groups.

Peru is a member of the United Nations, the Organization of Latin American States, and several other international security organizations. Peruvian intelligence services participate in ongoing international and domestic anti-drug trafficking and anti-terrorism operations.

## Peru, Intelligence and Security

Peru is the seat of the ancient Incan Empire, one of the most advanced indigenous civilizations in the Americas. Spanish conquistadors captured the empire in 1533. In 1921, Peru declared its independence.

In the last two decades of the twentieth century, Peru sought a stable government and a means of overcoming endemic economic woes. The 1990 election of Alberto Fujimori ushered in a brief era of prosperity and stability, but increasing accusations of corruption and authoritarianism undermined the legitimacy of the Fujimori government. He was ousted from power in November 2000. Although democratic elections were held in 2001, the Peruvian government continues to weather occasional political turmoil.

Intelligence and security services have existed in Peru since the era of the Incan Empire. In the modern era, Peru's intelligence community resembles that of neighboring nations, and takes an active, cooperative role in addressing regional intelligence and security issues.

The main civilian intelligence agency in Peru is the National Intelligence Service (SIN). The agency was restructured in 1990 to eliminate military influences and

#### ■ FURTHER READING:

#### ELECTRONIC:

Central Intelligence Agency. "Peru." CIA World Factbook. <<http://www.cia.gov/cia/publications/factbook/geos/pe.html>> (April 8, 2003).

### PET (Positron Emission Tomography).

SEE *Scanning Technologies*.

## Petroleum Reserves, Determination

#### ■ WILLIAM J. ENGLE

Petroleum reserves are the recoverable portion of hydrocarbon accumulations that exist below Earth's surface in traps or reservoirs. The quantification of these reserves is

essential to the world's effort to utilize hydrocarbons as a major energy source. The identification of petroleum reserves, both foreign and domestic, is an increasingly important scientific component of national economic and strategic security.

The process of quantifying reserves is governed by a host of scientific, political and economic considerations. Reserve determination is an interpretive process for which there is no finite answer until the end of a reservoir's producing life. Independent reserve estimates for the same asset base can vary significantly even though based on the same source data and with the application of prudent and customary technical methods. For general studies and large scale planning purposes statistical methods may be used to project reserves within an acceptable range of uncertainty, but specific projects beyond the earliest exploratory phase require at least a minimum of physical data. Uncertainty in reserve estimates is inversely proportional to the understanding of the producing characteristics of the accumulation and will remain a concern throughout the life of the project.

Uncertain reserve estimates for a reservoir or an entire project typically decrease over the life of a project as more factual information becomes known and actual production is observed.

Reserve estimates during the pre-drill exploratory phase are often based on known geologic factors from other areas thought to be sufficiently similar to the area under study applied to a reservoir description based on site specific interpretive data. In-place and recoverable reserve factors are applied to volumetric maps derived from seismic data and other geologic studies. The range of uncertainty at this time can be quite large. The actual existence of hydrocarbons has yet to be verified by actual well data and characterized as to their nature, quality, and economic viability. All studies at this point are speculative and highly dependent upon the creditability of the data available.

The first well drilled in the prospect enables project geologists and engineers to begin refining the assumptions used in the initial reservoir characterization efforts. Just how much this initial information improves the reserve estimate depends upon the degree and quality of data obtained. Each additional exploratory well adds more information and further refines the reserve estimates until it becomes possible to make a decision to go forward with project development or not based on an assessment of technical and economic risks. Ideally an actual flow test that includes a brief flow test of reservoir fluids and collection of fluid samples is conducted during this phase. However, this is not always done if confidence in other data more easily obtained is high and correlates well with the expected outcome, as flow testing can be quite expensive.

Each additional well, either as an expendable appraisal or a development well, further refines the data available and improves the interpretive understanding of

project potential and further reduces but does not eliminate uncertainty in the reserve estimate. Until actual sustained production is established, the reserve estimate remains a volumetric determination and is highly dependent on the accuracy of the reservoir description. Nonetheless, the decision to make the significant capital investments required for project development is often based on a risked assessment of reserve potential with much yet unknown.

First production is a significant step toward improving the quality of reserve estimates. With continued geologic and engineering study and surveillance of actual reservoir performance the assumptions used to make previous reserve estimates are further refined with greater confidence. The range of uncertainty in the reserve estimate continues to narrow with actual performance.

Considerations that must be taken into account when estimating reserves tend to fall into the four categories of geology, fluid behavior, reservoir mechanics, and economic and political considerations.

Many of the geological factors considered in making the estimate of in-place reserves have to be refined and described in considerably greater detail if their effects upon hydrocarbon recovery are to be understood. These factors include but are not limited to structural geometry, size, shape, rock composition and compressibility, porosity, permeability, and compartmentalization.

The reservoir must be thought of in its three-dimensional configuration (e.g., whether it is in the shape of a box, sphere, dune, or an ancient river channel or a beach; whether it spreads over a massive area or it is intermittently scattered; whether it is flat, tilted, or undulating). Other considerations include analysis of whether the rock is clean sand, a mixture of sand and shale, limestone, or a number of other potential rock types that behave differently. A fundamental question involves whether the rock will compress as reservoir pressure depletes with fluid withdrawal. The degree of rock porosity—and the degree of minute rock particles called "fines" that exist in the pore space—are important considerations in determining whether the well will flow smoothly. Without effective permeability, the reservoir is of limited value. Once these other factors are known, the critical issue of compartmentalization remains (e.g. whether the reservoir is broken into sub-compartments by structural fractures or variations in permeability or whether fractures are sealing so as to prevent fluid flow across them). Obviously the more actual well data in an area, the better able one is to answer these questions. Until such data is available, advanced interpretations of seismic surveys and geologic models will be made and refined as well data is incorporated into the process.

The character of the reservoir fluid itself is a critical factor. Geologists conduct specific tests to determine the in-place gas or liquid phase and to what degree the phase is affected by temperature and pressure changes. A gas phase has low viscosity and high mobility, while liquids

may have a viscosity ranging from that of water to that of solid asphalt. In calculating in-place reserves, the pore space saturation of other fluids is considered, most notably water but other potentially existing fluids such as carbon dioxide, nitrogen, hydrogen sulfide, elemental sulfur and others must be accounted for. The analysis of fluid and rock samples is critical.

Recovery is also dependent on which fluid actually wets the rock grain surface and to what extent resulting capillary pressures retain fluids within the rock matrix. These effects may restrict fluid flow through the porous rock media and govern how much of the original fluid saturation in-place can be recovered and how much will remain as residual saturation. Depending upon the lithology of the reservoir rock, residual gas saturation (i.e., the fraction of in-place gas that will remain in the reservoir) can range between 15 percent and 50 percent. For oil, residual saturation may range between 18 and 65 percent.

Reservoir mechanics are a major determining factor in hydrocarbon recovery and represent the energy that causes mobile fluids to flow through reservoir rock, also known as the drive mechanism. In a gravity drainage system, there is little pressure trapped within the bound fluid and the primary moving force is the pull of gravity on the density of the liquid. The resulting recovery is quite low, as may be demonstrated by fully wetting a sponge then lifting it out of the water with out squeezing it to see how much water runs out and how much is retained; then try this experiment with a more viscous fluid.

If reservoir fluids are under pressure, they may expand as pressure is released. This condition is an expansion drive and one in which the expanding fluid effectively flows from high pressure at the reservoir boundary to low pressure in the producing wellbore. Fluid recovery in an expansion drive is better than gravity drainage. The gas phase and recovery will tend to be a function of the real gas law where the relationship between changing pressure, temperature, and volume must be also adjusted for changing gas compressibility. Liquid recovery will be a function of fluid expansion. However, fluid recoveries are limited to their own ability to expand, thus an expansion or pressure depletion drive still leaves a considerable amount of hydrocarbon behind.

The highest yielding unassisted drive mechanism is a water drive system. In this case, the hydrocarbon bearing zone is in contact with a considerably larger body of water that can effectively push the hydrocarbon to the producing well(s) as the water itself expands as in a depletion drive. The strength of a water drive system is dependent on the size of the supply of water, or aquifer, and its relative energy potential or source. The larger the aquifer, the better the water drive. However the manner in which the water or "flood front" moves through the reservoir has great effect on its displacement of hydrocarbons. Irregularities in rock quality can cause channels to occur that may cause the moving water to have a low sweep-efficiency and possibly bypass large quantities of in-place hydrocarbons.

And of course a reservoir may exist in a combination of several drive mechanisms and each may dominate performance at different times in the life of the reservoir. Typically, under primary depletion, gas recoveries can range from as low as 50 percent to close to 90 percent of the original in-place volume. Oil recoveries will range between 5 percent and 35 percent and in some cases a little better. Artificial means of lifting fluids or adding energy to a reservoir with pumps, gas injection, or water injection as secondary recovery projects can increase recoveries to some extent. In less frequent occurrences, tertiary recovery techniques may be applied through several forms of miscible flooding with a fluid that will reduce the residual oil saturation left behind or going as far as starting a fire flood within the reservoir. However the incremental recoveries to be gained from secondary and tertiary recovery can be costly to put in place and have their own inherent uncertainties that must be closely monitored.

Economic and political considerations will also impact recoverable reserves. As a field declines, it will ultimately reach an economic limit beyond which it is impractical to continue producing operations. The economic limit is impacted by declining well productivity, higher maintenance expense late in the life of a field, changing commodity prices, taxation and the cost of employing technology, and complying with changing rules and regulations. Very often the economic limit is one of the most uncertain factors affecting ultimate recovery.

#### ■ FURTHER READING :

##### BOOKS:

Craft, B. C. *Applied Petroleum Reservoir Engineering*, 2nd ed. Englewood Cliffs, NJ: Prentice Hall, Inc., 1991.

##### SEE ALSO

*DOE (United States Department of Energy)*

---

## PFIAB (President's Foreign Intelligence Advisory Board)

---

#### ■ CARYN E. NEUMANN

The President's Foreign Intelligence Advisory Board (PFIAB) provides unbiased monitoring of the overall intelligence effort of the United States by continually reviewing the activities of agencies and departments engaged in intelligence work. Through briefings and visits to intelligence installations, the sixteen board members seek to identify deficiencies in the collection, analysis, and reporting of

intelligence while eliminating duplication. Created by President Dwight D. Eisenhower in 1956 as part of a reorganization of the executive branch, the board languished under President John F. Kennedy until the Bay of Pigs fiasco exposed the need for an objective evaluation of intelligence efforts. The board has served all subsequent presidents.

The PFIAB began when the 1955 Hoover Commission on Organization of the Executive Branch of the Government recommended that the president appoint a committee of knowledgeable private citizens to examine and report to him periodically on American foreign intelligence efforts. Accordingly, on February 6, 1956, Eisenhower issued an executive order establishing the President's Board of Consultants on Foreign Intelligence Activities (PBCFIA). The board focused on the quality of training and personnel, security, progress in research, effectiveness of specific projects, and general competence in carrying out assigned tasks.

Eisenhower left office in 1960 and Kennedy declined to appoint new PBCFIA members. Meanwhile, the new president had inherited a plan, approved by Eisenhower, for the invasion of Cuba. The CIA and most military advisors assured Kennedy that the plan was sound, but the Cubans anticipated the Bay of Pigs attack and defeated the American-backed forces within three days. Amidst widespread international condemnation and a humiliating loss of national prestige, Kennedy reinstated the board, now named PFIAB, to prevent another embarrassing disaster. Kennedy placed Clark Clifford (1906–98), the man who had written the 1947 legislation establishing the CIA, upon the board and later made him chair. President Jimmy Carter replaced the board in 1977 with the smaller Intelligence Oversight Committee as part of a reevaluation of intelligence gathering. President Ronald Reagan brought the PFIAB back to life in 1982.

The activities and deliberations of the PFIAB have remained classified. However, it is known that the PFIAB expressed particular concern with the internal procedures of the CIA. It also examined the delay in receiving information about the installation of Soviet offensive nuclear missile sites in Cuba. These sites, which precipitated the Cuban Missile Crisis, had been discovered in 1962 by a U-2 spy plane that had been aided in development by the PFIAB. Technical collection programs, like the one that produced the U-2, are heavily monitored by PFIAB as part of its interest in ensuring that intelligence technology reflects the best technical capabilities of the nation. Lastly, it is also known that the board investigated the U.S. government's failure to predict the 1968 Soviet invasion of Czechoslovakia, which had been decided upon at a meeting of Warsaw Pact nations concerned about the threat that proposed Czech reforms posed to the preservation of the communist system. The board has very rarely addressed covert political action.

The PFIAB conducts deliberations every two months for two days. Chairs of the board have included Clifford; retired Army General Maxwell D. Taylor (1901–87), former

Chairman of the Joint Chiefs of Staff who succeeded Clifford from 1968–70; retired Admiral George W. Anderson, Jr., Chief of Naval Operations under Kennedy, 1970–76; Anne L. Armstrong, former Ambassador to the United Kingdom, 1982–90; Warren Rudman, former U.S. Senator, 1997–2001, and current chair, retired Air Force Lieutenant General Brent Scowcroft. The history of intelligence disasters and the importance of good information to national security likely guarantees that the PFIAB will continue to monitor intelligence efforts.

#### ■ FURTHER READING:

##### BOOKS:

Congressional Research Service. *The United States Intelligence Community: A Brief Description of Organization and Functions*. Washington, D.C.: Library of Congress, 1975.

Hoxie, R. Gordon. et al. *The Presidency and National Security Policy*. New York: Center for the Study of the Presidency, 1984.

Marchetti, Victor, and John Marks. *The CIA and the Cult of Intelligence*. New York: Alfred A. Knopf, 1974.

##### ELECTRONIC:

The White House. "President's Foreign Intelligence Advisory Board." <<http://www.whitehouse.gov/pfiab/>> (March 29, 2003).

##### SEE ALSO

*Air Force Intelligence, United States Aviation Intelligence, History*  
*Carter Administration (1977–1981), United States National Security Policy*  
*CIA (United States Central Intelligence Agency)*  
*CIA, Formation and History*  
*Cuban Missile Crisis*  
*Eisenhower Administration (1953–1961), United States National Security Policy*  
*Executive Orders and Presidential Directives*  
*Johnson Administration (1963–1969), United States National Security Policy*  
*Kennedy Administration (1961–1963), United States National Security Policy*  
*President of the United States (Executive Command and Control of Intelligence Agencies)*  
*Reagan Administration (1981–1989), United States National Security Policy*  
*United States, Intelligence and Security*  
*United States Intelligence, History*

---

## Phoenix Program

---

In an attempt to cripple or eliminate South Vietnamese communist guerilla resistance (the Vietcong) to both United States forces and the U.S.-backed government of South

Vietnam, the Phoenix program was allegedly designed to conduct arrest and assassination operations against suspected Vietcong and Vietcong sympathizers. The Phoenix program was developed and operated by the United States Central Intelligence Agency (CIA), the United States Army, and components of several South Vietnamese intelligence and law enforcement agencies.

U.S. CIA personnel (including those assigned to Intelligence Coordination and Exploitation operations) provided the core of Phoenix leadership. Starting in 1967, the program, which was based in Saigon (then the capital of South Vietnam) used a complex network of informants, a mix of military intelligence, and even trials at computer algorithms to determine appropriate targets for “neutralization.” In 1968, CIA officer William Colby (who would become Director of Central Intelligence in 1973) assumed command of the program.

Initially named the Phuong Hoang Operation (named after a mythical Vietnamese bird of prey), the renamed Phoenix program resulted in the arrest, detention, brutal interrogation, and execution of thousands of Vietcong fighters and sympathizers at the hands of South Vietnam police and intelligence agencies. In addition to identifying suspected Vietcong and Vietcong sympathizers, Phoenix intelligence operations also accumulated data that exonerated thousands of suspects. Phoenix operations, and the identification of Vietcong infrastructure became increasingly important after the 1968 Tet Offensive and Phoenix generated intelligence was used to determine military targets.

## ■ FURTHER READING:

### BOOKS:

Colby, William E., and James McCargar. *Lost Victory: A First Hand Account of America's Sixteen-year Involvement in Vietnam*. Chicago, IL: Contemporary Books, 1989.

Moyar, M. *Phoenix and the Birds of Prey: the CIA's Secret Campaign to Destroy the Viet Cong*. Annapolis, MD: Naval Institute Press, 1997.

## Photo Alteration

The camera was invented in 1839, and by the next decade, photographers had already begun to manipulate photographic images. Initially, the manipulation was part of the exploration of the artistic potential of the new medium. Soon, the informational power of the photograph became recognized.

The techniques of photo alteration have been exploited to generate images that are different from the

actual scene that is photographed for purposes of intelligence gathering or deception. For example, by the 1940s, the Soviet Union was actively manipulating photos in a campaign of misinformation to portray their leaders favorably.

In the intelligence and security communities, photo alteration serves two important purposes. The first purpose is to gather information, most often through magnification of photos. The use of spy satellites reveals facilities and operations that can be crucial to national security. One example is the famous photos of a Soviet rocket installation in Cuba during the presidency of John F. Kennedy. In the modern era, satellite photos purporting to show biological weapons production facilities have increased the resolve of the United States to topple the government of Iraq. The ability to produce photographs that reveal more detail than do traditional photographs, especially at longer distances or using small cameras, has increased the information that can be gathered.

The second purpose of photo alteration is to misinform or deceive. With new technology, the ability to alter a photographic image is easier than ever before. For example, in a traditional photograph, the difference in skin tone between a face and the neck or shadows that point in different directions can be clues that an image has been manipulated. However, these visual discrepancies can be eliminated in the digital image. Thus, the ability to generate false or misleading information has become routine.

**Traditional photo alteration.** In the days before digital technology, photo alteration was accomplished in the darkroom during the development and printing of the photograph. In a technique called dodging, the light shining through the photographic negative onto light-sensitive paper was obscured. Because less light strikes the paper, that region appears lighter in the developed image. In contrast, the technique of burning allows an increased amount of light to strike the photographic paper. The result of burning is to make the region appear darker in the print.

The traditional techniques of dodging and burning are used to enhance or disguise aspects of the photo. As well, details can be excluded from an image by the use of cropping, where only the selected portion of the image is printed. Photographs can also be enlarged to selectively print portions of the image. Enlarging cannot be done indefinitely, however, since the eventual inability to separate the informational components of the image from one another produces a blurry picture.

A skilled technician can even paint a picture to remove someone, replacing the person with the background. Photographing the altered image produces an image that can often pass for the real thing. A classic example of this manipulation is the picture of Vladimir Lenin addressing a crowd in front of Moscow's Bolshoi Theater in 1920. In



Senator Joseph McCarthy answering charges that the photo, foreground, submitted as an exhibit at Army dispute hearings in 1954, had been altered. AP/WIDE WORLD PHOTOS.

reality, Leon Trotsky was also on the film. In a massive campaign of historical revisionism during the leadership of Joseph Stalin, Trotsky's involvement in this and other photographed events was erased in an attempt to purge the memory of opposition to Stalin's leadership.

Another ploy of photo manipulation is the false captioning of an image. By excluding, exaggerating, or falsifying details of an image, the viewer can misinterpret what is seen. For example, during World War II the United States plowed fields on some South Pacific Islands, then took aerial photos of them. The photos were labeled as representing air bases, creating a deception that the military resources in the area were much more extensive than was actually the case.

**Digital photo alteration.** The coming of digital photography revolutionized the ability to alter photographs. The laborious darkroom manipulations of preceding times could be accomplished by a few commands in specialized photographic software.

In traditional photography, the reflected light from the subject enters the camera through the lens and is focused onto the surface of a light-sensitive emulsion. The emulsion records the image, which can be beamed onto light-sensitive photographic paper. The paper is subsequently treated with chemicals to make the image appear. It is during this latter printing process that the alteration of the photograph can be accomplished.

In digital photography, the reflected light that enters the camera is focused onto a chip that is known as a charged coupling device (CCD). The surface of the CCD contains an array of light-sensitive photo diodes. Each diode represents a pixel (the basic unit of programmable color in a computer image). Each photo diode is hooked up to a transistor, which sends an electrical signal (whose voltage corresponds to the light intensity that registered on the photo diode) to another chip. The second chip converts the electrical signal to digital information—1s and 0s—that can be interpreted by computerized photo manipulation software programs.



Colors are assigned a code sequence between 0 and 255; 0 is black and 255 reveals the most intense shade of red possible by the software. These coded assignments are in turn converted to sequences of 0s and 1s. Black, for example, is 00000000, while the most intense red is 11111111. Shades in between are combinations of 0s and 1s in the eight-digit sequences.

Digital photo manipulation involves the alteration or elimination of the digital 1s and 0s. Changing an eight-digit sequence is trivial. When the digital information is reconstructed into an electronic image, the result can be an altered color.

In addition to color change, a myriad of effects are possible, including color enhancement, elimination of regions of the image, increased contrast, correction of a blurred image, and the merging of other images with the original image (a photographic version of the “cut and paste” operations in word processing).

As digital photo manipulation software has increased in technical sophistication, and people have become more adept at using the software, the task of detecting manipulated images has become very challenging. Digital photographic manipulation is now so sophisticated that it can sometimes be impossible to discern whether people or objects in a photograph were actually there when the photo was taken. This has spurred efforts, especially in the military and intelligence communities, to establish a system of image verification. In this regard, the United States Air Force Research Laboratory in Rome, New York, has developed a technique called digital watermarking. Akin to the watermarking of paper currency to establish authenticity, digital watermarking embeds an encrypted image over the actual photo image. The encrypted image is invisible to the naked eye, but can be detected by specially designed image scanners. The lack of the digital watermark is evidence of an altered image.

Digital cameras can also be mounted in satellites in orbit hundreds of miles above the Earth. These cameras can provide images that can be manipulated to allow objects that are as close to one another as a meter or two to be visually distinguished from each other. This resolution is a vast improvement from that possible using traditional light-sensitive photographic film. This form of digital photo manipulation has improved the capability of intelligence agencies to spy on other countries or organizations from a long distance.

In the U.S., government scrutiny and interpretation of photographs is the function of the National Imagery and Mapping Agency’s National Photographic Interpretation Center (once part of the Central Intelligence Agency’s Directorate of Science and Technology).

#### ■ FURTHER READING:

##### BOOKS:

Beale, Stephen. *Web Tricks and Techniques: Photo Manipulation: Fast Solutions for Hands-On Web Design*. Gloucester, MA: Rockport Publishers, 2002.

Brugioni, Dino A. *Photo Fakery: The History and Techniques of Photographic Deception*. Washington, D.C.: Brassey’s, 1999.

##### SEE ALSO

*Computer Modeling*  
*Document Forgery*

---

## Photographic Interpretation Center (NPIC), United States National

---

The Central Intelligence Agency (CIA) established the National Photographic Interpretation Center (NPIC) in the 1950s to provide skilled interpretation of photographic images obtained by low- and high-flying aircraft, and later by satellites. Originally a unit of the CIA Directorate of Intelligence, NPIC in 1973 transferred to the Directorate of Science and Technology (DS&T). In 1996, it was moved to the newly formed National Imagery and Mapping Agency (NIMA).

An intelligence photograph, rather like the sonogram of an unborn baby, seldom yields an abundance of secrets to the untrained eye. An expectant parent is unlikely to guess the sex of the child from a sonogram photo, whereas an experienced practitioner can ascertain such information with a high degree of certainty. Similarly, an aerial image of a military installation may appear, to the layman, as no more than a grid of fuzzy rooftops and curving roads, whereas a specialist skilled at extracting intelligence from photography may see all manner of incriminating details.

Americans became more acquainted with photographic interpretation on February 5, 2003, when Secretary of State Colin Powell presented NIMA/NPIC imagery to the United Nations (UN) Security Council as proof that Iraqi dictator Saddam Hussein was stockpiling chemical weapons in defiance of international bans. Likewise, NPIC played a critical role in a much earlier international situation, that of the Cuban Missile Crisis of October 1962.

The center’s analysts had been studying photos taken from U-2s over the Soviet Union since July 1956, and over Cuba since October 1960, but it did not officially come into existence until President Dwight D. Eisenhower signed National Security Council Intelligence Directive No. 8 on January 18, 1961. As the Soviets began sending arms and other supplies to Havana during the early days of John F. Kennedy’s administration, NPIC personnel attempted to measure—and, if possible, identify the contents of—each crate unloaded on the docks. Kennedy relied heavily on

NPIC, as well as Defense Department equivalents in the navy and air force. During the crisis, he dispatched emissaries, bearing NPIC photographs as proof, to several U.S. allies before he confronted Soviet premier Nikita Khrushchev with evidence of the buildup in Cuba.

■ FURTHER READING :

PERIODICALS:

Munro, Neil. "Fighting for Intelligence Funds." *Washington Technology* (July 27, 1995): 1.

Pincus, Walter. "CIA, Pentagon Back NIMA 'Concept,' Combining Spy Satellite Photo Units." *Washington Post*. (November 29, 1995): A23.

Seffers, George I. "NIMA 'Inadequate' in Analyzing Spy Data." *Federal Computer Week* 15, no. 3 (February 5, 2001): 55.

ELECTRONIC:

National Photographic Interpretation Center. Fellowship of American Scientists. <<http://www.fas.org/irp/overhead/npic.htm>> (February 13, 2003).

SEE ALSO

*CIA Directorate of Science and Technology (DS&T)*  
*NIMA (National Imagery and Mapping Agency)*  
*Photographic Resolution*  
*Photography, High-Altitude*

## Photographic Resolution

The term resolution, in the context of photography, refers to the degree to which adjacent objects can be distinguished from one another in a photographic image. Obviously, the higher the degree of resolution—which is a function of the acuity of the photographic equipment used, as well as the abilities of the operator—the better the quality of the photograph. The lower the figure given for the resolution, in metric or English units, the higher the degree of resolution.

For example, the first four satellites of the CORONA project, which remained aloft throughout most of the period from June 1959 to December 1963, had a relatively high resolution of 25 feet (7.6 m), meaning that objects smaller than that size were likely to be indistinguishable from one another. Higher still was the resolution of the fifth satellite in the series, KH-4B (September 1967-May 1972), at 6 feet (1.8 m). Photographs taken by KH-5, a satellite deployed for mapping purposes between February 1961 and August 1964, had a much lower degree of photographic resolution: 460 feet (140 m).

■ FURTHER READING :

BOOKS:

Williams, John B. *Image Clarity: High-Resolution Photography*. Boston: Focal Press, 1990.

ELECTRONIC:

Declassified Intelligence Satellite Photographs. <<http://mac.usgs.gov/isb/pubs/factsheets/fs09096.html>> (February 13, 2003).

SEE ALSO

*Cameras*  
*Photography, High-Altitude*

## Photography, High-Altitude

The United States conducts, and has conducted, operations in high-altitude photography for a number of purposes. In addition to intelligence-gathering operations such as that of the CORONA program in the 1960s, civilian undertakings such as those of the U.S. Geological Survey (USGS) have an obvious, if unspoken, intelligence application. High-altitude photography, which offers several advantages over ground-based surveillance, has evolved over the years, along with the equipment: from balloons to prop planes, jets, and satellites.

### High-Altitude Photography and its Applications

High-altitude photography enables the coverage of large areas—for example, a military installation—in a single photographic frame. For a larger region such as a metropolitan area or state, it may be necessary to form a mosaic of several photographs. The more sophisticated the photographic equipment, the more the area that can be portrayed with a reliable degree of photographic resolution.

The same goes for the technology necessary to keep the camera aloft: a satellite, because it orbits at a considerably greater height than the highest-flying plane, by definition possesses a much better vantage point for breadth of coverage. The July 1976 issue of *National Geographic*, which commemorated the U.S. bicentennial, illustrated this breadth dramatically with a fold-out aerial photograph of the United States patched together from hundreds of satellite photographs.

**From balloons to satellites.** In the mid-nineteenth century, European and later American armies began using balloons as observation platforms. From this it was a logical step to mount camera equipment on the balloons. The

advent of the airplane as an instrument of both combat and surveillance was all but concurrent with the use of photographic equipment for intelligence purposes. By the end of World War I, the use of high-altitude craft for the gathering of photographic intelligence was firmly established.

The use of airplanes in surveillance did not rule out the application of balloons. These included both ordinary balloons, which had made their debut in the late eighteenth century, as well as airships, or guided balloons, pioneered in the last third of the nineteenth century. As late as 1956, the U.S. Air Force was using balloons in Project GENETRIX, a failed effort to conduct surveillance of Eastern Europe, the Soviet Union, and the People's Republic of China.

Yet the age of the jet and the satellite was well under way by then. Already the Central Intelligence Agency (CIA) was putting the finishing touches on its plans to employ the high-speed U-2 aircraft for overflights of the Soviet Union and other countries, and in 1957, the Soviets themselves launched the first artificial satellite, *Sputnik*.

**Satellites.** In the years since, the United States has used satellites in a number of information-gathering capacities. Significant among these operations was CORONA, which involved the launch of some 145 satellite flights between 1960 and 1972. CORONA collected some 800,000 images, most of which covered an area about 10 miles (16 km) wide and 120 miles (193 km) long. Resolution was accurate for objects as small as 6.6 feet (2 m).

CORONA operations took place before the era of digital imaging, and therefore images had to be sent back to Earth manually, by means of film capsules attached to parachutes and retrieved by an Air Force C-119. Information gathered by the CORONA systems, which were designated KH-1, KH-2, KH-3, KH-4A, and KH-4B by the intelligence community, was declassified by Executive Order 12958 in 1995. Today USGS controls most of the images.

**USGS photographic operations.** A unit of the Department of the Interior, USGS is responsible for measuring and mapping areas of Earth's surface, particularly those in the United States; for managing resources; and for minimizing threats to life and property by identifying hazards. Although USGS is ostensibly outside the security and intelligence component of the federal government, its application in those areas is clear. Among its undertakings is the Military Geology Project, which is primarily concerned with monitoring nuclear tests, and breaches of nuclear treaties, worldwide.

Geologists make extensive use of remote sensing, or the gathering of data without actual contact with the materials or objects being studied. High-altitude photography is among the most significant techniques of remote

sensing, and USGS has used airplanes and satellites for a number of projects.

Among these was the National High Altitude Photography Program (NHAP), launched in 1980 to collect aerial photographic images of the 48 conterminous states every five to seven years. Undertaken in an effort to eliminate duplication of government mapping programs, NHAP in 1987 became the National Aerial Photography Program (NAPP). NHAP acquired photographs at 40,000 feet (12,190 m), and NAPP at half that altitude. Both used a 6-inch focal length lens, which for NHAP obtained black-and-white pictures and for NAPP either color infrared or black-and-white. NHAP also used an 8.25-inch lens to obtain color infrared images.

At a much higher altitude, USGS has also been one of the principal agencies involved in the Landsat satellite program, which began with the launch of Landsat 1 in 1972 and continued in the early twenty-first century with Landsats 5 and 7. Tasked primarily with providing information on environmental hazards and natural disasters, Landsat 7 orbits the planet every 99 minutes. Its photographic equipment, while noted for its high spatial resolution—98 feet (30 m)—in comparison to that of other scientific satellites, is of relatively low resolution compared to that of intelligence satellites such as CORONA three decades earlier.

**Overflights.** Even with satellites in space, the United States has continued to employ overflights, or missions by spy planes over enemy countries to collect intelligence via electronic or photographic equipment. The concept of the overflight, which involves the gathering of information on strategic activities in the country rather than the tactical activities of its enemy forces, dates back at least to 1952, when the United States sent B-47 Stratojets over Soviet airspace.

Perhaps the most well known use of overflights was that of the U-2 over the Soviet Union, a fact that came to world attention when pilot Francis Gary Powers was shot down in 1960. Though it made its debut in 1955, the U-2 was still being used in 2003, as part of United Nations weapons inspector's work in Iraq. Even in the early 1960s, the photographic equipment aboard the U-2 was exceptional: its camera had a 944.7-millimeter lens, and was capable of capturing an area measuring some 125 miles (201 km) by 2,174 miles (3,499 km) in 4,000 photographs.

The SR-71 Blackbird made its debut in 1964, when it was presented as a successor to the U-2. In fact the two flew concurrently, and the U-2 remained in the skies during a period from 1990 to 1995, when the SR-71 was mothballed due to its high costs of operation. Much faster and higher-flying than the U-2, the SR-71 has been used to photograph operations in enemy countries ranging from China and North Vietnam to Libya and Iraq to Cuba and the communist Nicaragua of the 1980s. An SR-71 photographed China's first hydrogen bomb explosion in 1967.

## ■ FURTHER READING :

### BOOKS:

Barrett, E. C., and L. F. Curtis. *Introduction to Environmental Remote Sensing*. New York: Chapman & Hall, 1992.

Walker, James W., and Steven Leroy De Vore. *Low Altitude Large-Scale Reconnaissance: A Method of Obtaining High Resolution Vertical Photographs for Small Areas*. Denver, CO: Interagency Archeological Services, National Park Service, 1995.

### ELECTRONIC:

Declassified Intelligence Satellite Photographs. <<http://mac.usgs.gov/isb/pubs/factsheets/fs09096.html>> (February 13, 2003).

United States Geological Survey. <<http://www.usgs.gov>> (February 13, 2003).

### SEE ALSO

*Balloon Reconnaissance, History*  
*NIMA (National Imagery and Mapping Agency)*  
*Photographic Interpretation Center (NPIC), United States National Reconnaissance*  
*Satellites, Non-Governmental High Resolution Satellites, Spy*

## Playfair Cipher

The Playfair cipher is a method of cryptography invented in 1854 by English physicist Sir Charles Wheatstone (1802–1875). The encryption method was named for Wheatstone’s friend, Lyon Playfair, who helped popularize the cipher by successfully lobbying for its official adoption by the British government.

All cryptography schemes are designed to conceal a message’s meaning and maintain confidentiality in communications. The Playfair is a block cipher that disguises a message by substituting each pair of letters in the plaintext with a secondary pair of letters. Each unit or pair of letters is known as a digraph.

A keyword, usually only known to the sender and recipient, is written into a five-by-five square. Repeated letters are omitted. After the keyword is spelled out, empty blocks are filled with the rest of the letters of the alphabet in alphabetical order. The letters I and J are treated as the same letter and therefore, combined in the same block. The following example is a Playfair cipher decoded by Lord Peter Wimsey in Dorothy L. Sayers’s *Have His Carcase*. The keyword is “Monarchy.”

Enciphering the phrase, “We are discovered. Save yourself,” involves several steps. First, the plaintext is

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

divided into two-letter groups. An X is added when there is an uneven number of letters.

WE AR ED IS CO VE RE DS AV EY OU RS EL FX

Next, locate the position of the two plaintext letters in the box matrix. Letters appearing in different rows and columns are replaced by the letter that is in the same row but in the other column; i.e., to encrypt WE, replace W with U, and E by G.

When a pair appears in the same row, as A and R does above, each letter is encrypted as the next cyclically appearing letter; i.e., AR becomes RM. The same rule of thumb applies when the pair is in the same column. In this example, IS would be encrypted as SX.

The enciphered phrase for Sayers’s Playfair becomes:

UG RMK CSXHMUFMKB TOXG CMVATLUIV

In the event a double letter occurs, a bogus letter, such as an X, replaces the repeating letter. In order to decrypt the message, simply reverse the process.

The simplicity and reliability of this primitive code-cracking method made it extremely popular on the battlefield. The British employed the Playfair in the Boer War in addition to World War I. Several militaries relied on the Playfair as a back-up cipher during the Second World War. Lieutenant (and later, President) John F. Kennedy used the Playfair encryption method to send an emergency message after his PT-109 sank in the Solomon Islands in 1943.

## ■ FURTHER READING :

### ELECTRONIC:

University of North Dakota. “The Cipher Exchange and Cipher Standards.” <<http://www.und.nodak.edu/org/crypto/crypto/.chap08.html#PLAYFA>> (December 09, 2002).

Glyphworks. "Classical Cryptography." <[http://storm.prohosting.com/~glyph/crypto/class\\_sub.shtml](http://storm.prohosting.com/~glyph/crypto/class_sub.shtml)> (December 09, 2002).

NOVA Online. "The Playfair Cipher." November 2000. <<http://www.pbs.org/wgbh/nova/decoding/playfair.html>> (December 14, 2002).

#### SEE ALSO

*Cryptology and Number Theory*  
*FISH (German Geheimschreiber Cipher Machine)*

---

## Plum Island Animal Disease Center

---

The Plum Island Animal Disease Center (PIADC), located on a 180-acre site off the northeastern tip of Long Island, New York, is part of the Department of Homeland Security's efforts to protect the United States food supply. PIADC works to protect U.S. consumers and safeguard the integrity of U.S. animal product exports against biologic agents introduced accidentally or deliberately introduced by terrorists.

PIADC scientists protect American livestock by developing methods to identify and isolate foreign animal diseases. PIADC scientists have developed testing, containment, and treatment protocols for a range of foreign animal diseases including foot-and-mouth disease, African swine fever, and African horsesickness. PIADC researchers are specifically responsible for developing a number of antiviral drugs and vaccines for foreign animal diseases and for the development of disease-specific nucleic-acid-based probes that serve in diagnostic tests.

For example, PIADC researchers discovered and developed a synthetic DNA copy of the genetic information contained in the foot-and-mouth disease virus. Further research into the enzyme biochemistry of the virus responsible for foot-and-mouth disease has allowed vaccines to be designed in such a way to enhance vaccine storage. PIADC research also aims to perfect existing vaccines, for example developing enzyme-linked immunosorbent assay (ELISA) tests for foot-and-mouth disease variants that can be used outside the laboratory (i.e., in field tests) because the test does not contain live virus. In standard ELISA tests an enzyme or a radioisotope is covalently linked to the pure antigen or antibody. The unlabeled component, which most often is the antigen, is attached to the surface of a plastic well. The labeled antibody is allowed to bind to the unlabeled antigen. The plastic well is subsequently washed with plenty of buffer that will remove any excess non-bound antibody and



The Plum Island Animal Disease Center in Plum Island, New York, is shown in an aerial view. Researchers at the facility focus on animal diseases that can affect the health, security, and economic interests of the United States, such as the prevention of a foot-and-mouth disease outbreak introduced into the country by foreign livestock and travelers.  
AP/WIDE WORLD PHOTOS.

prevent non-specific binding. Antibody binding is measured as the amount of radioactivity retained by the coated wells in radioimmunoassay or as fluorescence emitted by the product of an enzymatic reaction.

PIADC scientists also sequenced (i.e., determined the specific sequence of nucleic acids) the DNA of the African Swine Fever virus, which, as of March 2003, was the largest animal virus ever sequenced. The work at PIADC allowed researchers to compare the genome of the African Swine Fever virus with the genomes of the human immunodeficiency virus (HIV) and human herpesvirus 6. The genomic comparisons provided evidence that the disease (African Swine Fever) was not causally related to either HIV or human herpesvirus 6 infections.

PIADC cooperates with industry to produce livestock vaccines. In addition, PIADC personnel conduct diagnostic investigations for suspected cases of foreign or emerging animal diseases and train veterinarians and other animal health professionals in the diagnosis of foreign animal diseases.

PIADC facilities operate at or above Biosafety Level 3 (BSL-3) standards, and general safety protocols require the use of airlocks, HEPA (High Efficiency Particulate Air)

filters, and other specialized vents and filters that remove any virus particles from air leaving the laboratory. Materials leaving laboratories are decontaminated, with waste products incinerated or specially heat-treated to kill viruses. The relative isolation of PIADC's setting and scientific containment facilities allow high confidence in the safety of pathogen storage and testing at PIADC. As of March, 2003, PIADC had never recorded a loss of pathogen containment. PIADC research supports work carried out by the United States Department of Agriculture (USDA) Agricultural Research Service and the USDA Animal and Plant Health Inspection Service.

#### ■ FURTHER READING:

##### ELECTRONIC:

Plum Island Animal Disease Center. <<http://www.ars.usda.gov/plum/index.html>> (March 23, 2003).

United States Department of Energy, Office of Science. National Laboratories and User Facilities. <[http://www.sc.doe.gov/Sub/Organization/Map/national\\_labs\\_and\\_userfacilities.htm](http://www.sc.doe.gov/Sub/Organization/Map/national_labs_and_userfacilities.htm)> (March 23, 2003).

United States Department of Homeland Security. Research & Technology. <<http://www.dhs.gov/dhspublic/display?theme=27&content=374>> (March 23, 2003).

##### SEE ALSO

*Argonne National Laboratory*  
*Brookhaven National Laboratory*  
*DOE (United States Department of Energy)*  
*Environmental Measurements Laboratory*  
*Lawrence Berkeley National Laboratory*  
*Lawrence Livermore National Laboratory (LLNL)*  
*Los Alamos National Laboratory*  
*NNSA (United States National Nuclear Security Administration)*  
*Oak Ridge National Laboratory (ORNL)*  
*Pacific Northwest National Laboratory*  
*Sandia National Laboratories*

## Plutonium Production.

SEE *Nuclear Reactors.*

## Poland, Intelligence and Security

Germany's invasion of Poland was the catalyst for World War II. During the Nazi occupation, Polish citizens were subject to interrogation and torture at the hands of officers of the Gestapo, the Nazi secret police. Holocaust death camps were located in occupied Poland. After the war, Poland became a Soviet satellite nation. The fall of the

Berlin Wall in 1989 opened Poland to the west. The following year, elections swept the labor union based Solidarity party into power. Poland then began the long process of democratizing the government and reforming the economy.

Before World War II, Poland had one of the strongest intelligence forces in Europe. The work of Polish spies and cryptographers broke several key German codes before the outbreak of the war. Fleeing Poland during the invasion, Polish agents successfully smuggled code breaking information and a German Enigma cipher machine to British Military Intelligence. Polish intelligence information directly aided British cryptography efforts at Bletchley Park.

Poland's Ministry of Internal Affairs governs domestic intelligence and security operations that relate to national security issues. In June 2002, the government dissolved the Office of State Protection (UOP). Though the organization was created after the fall of the communist regime, it failed to overcome public fears about its close association with former communist intelligence services and secret police forces. Two new agencies were established, the Domestic Security Office and the Intelligence Service. The Domestic Security Office works with law enforcement to protect diplomats, government officials, and national assets. The Intelligence Service directs most civilian intelligence operations, including counter-intelligence and counter-espionage.

Poland maintains an army, navy, and air defense force. Each military branch of service employs its own specially trained intelligence units. Operations that utilize military forces and government intelligence personnel, however, are supervised by the National Security Council (RBN) or a joint intelligence council. The Ministry of National Defense governs the Military Information Service, the electronic, signals, and communications intelligence agency.

While most of Eastern and Central Europe is still struggling with economic reform, Poland's government-driven rapid revitalization program has yielded the most robust economy in the region. Poland joined the North Atlantic Treaty Organization (NATO) in 1999, and is currently pursuing membership in the European Union (EU).

#### ■ FURTHER READING:

##### BOOKS:

Snyder, Timothy. *The Reconstruction of Nations: Poland, Ukraine, Lithuania, Belarus, 1569–1999*. New Haven, CT: Yale University Press, 2003.

##### SEE ALSO

*Bletchley Park*  
*European Union*  
*NATO (North Atlantic Treaty Organization)*  
*Ultra, Operation*  
*World War II*

# Politics: The Briefings of United States Presidential Candidates

■ JUDSON KNIGHT

In accordance with a practice established by President Harry S. Truman, presidential nominees of both major political parties receive intelligence briefings at some point between the summer political conventions and the presidential elections every four years. Assuming a candidate is an incumbent president or vice president, he is already accustomed to receiving such briefings, but for a contender who has not served in the inner circles of a previous administration, the briefing is an entirely new experience. The pace of briefings intensifies once a candidate is chosen in the November elections, and continues in the period leading up to inauguration day. Thereafter, the new chief executive will receive intelligence briefings on a regular basis in the form of the presidential daily briefing (PDB).

## Who Receives Briefings

Lyndon B. Johnson, Richard M. Nixon, Gerald R. Ford, and George H. W. Bush had all served as vice presidents, and therefore had received intelligence briefings while holding the nation's second-highest office. The same was true of several ultimately unsuccessful candidates for the presidency, including Nixon in 1960, Hubert Humphrey in 1968, Walter Mondale in 1984, and Albert Gore in 2000. Additionally, there had been several instances in which an incumbent ran for reelection and was defeated, meaning that in the period between November of election year and January of the following year, the successful challenger received intelligence briefings even as the sitting president received PDBs. Such was the case with Ford in 1976, James E. Carter in 1980, and Bush in 1992.

The system of intelligence briefings extends only to candidates of major parties. Although H. Ross Perot garnered more than 20 million votes in 1992, no serious consideration was given toward the idea of providing him with highly sensitive materials on national security and intelligence.

**Anatomy of the briefing system.** The career of George H. W. Bush, which included service as director of the Central Intelligence Agency (CIA), which administers the briefings, and later as vice-president and president, placed him in several interesting circumstances with regard to briefings. In 1976, he personally provided briefings to Carter, and in

1980 helped arrange briefings for Ronald Reagan, who had defeated him in the Republican primaries, and on whose ticket he was now running as vice-president.

In 1992, Bush was running for reelection as president against then-Arkansas governor William J. Clinton. After the latter received the nomination at the Democratic Convention, National Security Adviser Brent Scowcroft contacted Washington attorney Samuel Berger (who would hold Scowcroft's position in the second Clinton administration) to arrange briefings. CIA director Robert Gates traveled to Little Rock to personally brief Clinton and vice-presidential candidate Gore.

**Clinton's briefings in 1992.** The first briefings, on September 4, 1992, concerned the major national security issues of the moment, including turmoil in the soon-to-be-defunct Soviet Union and escalating conflict in Yugoslavia. Clinton received no further briefings until after the election, at which point a CIA team established a presence in Little Rock. Leading the briefings from that point onward was John L. Helgerson, who latter wrote *Getting to Know the President: CIA Briefings of Presidential Candidates, 1952–1992*, published by CIA's Center for the Study of Intelligence in 1996.

On November 11, Helgerson met with Clinton, Berger, and Nancy Soderberg of the governor's staff. Two days later, he began his briefings with Clinton. As Helgerson explained to the candidate, the PDB goes to the vice-president, national security advisor, chairman of the Joint Chiefs of Staff, White House chief of staff, and secretaries of State and Defense. In view of the growing importance of economic issues, Helgerson suggested that the Secretary of the Treasury also be included. Clinton agreed.

Other than this one suggestion, Helgerson indicated, he was hesitant to guide the president-elect in any way. Helgerson recalled that, in view of what he described as CIA "policy buzz saws" of the 1980s (most notably, the Iran-Contra scandal), he took great pains not to try to influence Clinton's thinking on any issues. Over the period from November 13 to January 16, 1993, Helgerson and others provided the president elect with daily briefings while Bush, now a "lame duck" president, received exactly the same material in his PDB. Beginning January 17, the briefing team moved from Little Rock to Washington, preparing to make the transition to providing Clinton with daily briefings as president.

## ■ FURTHER READING:

### BOOKS:

Helgerson, John L. *Getting to Know the President: CIA Briefings of Presidential Candidates, 1952–1992*. Washington, D.C.: Central Intelligence Agency, 1996.

### PERIODICALS:

Auerbach, Stuart. "Party Nominees to Get Trade Briefing." *Washington Post*. (June 25, 1988): D12.

## SEE ALSO

*CIA (United States Central Intelligence Agency)*  
*CIA, Legal Restriction*  
*Iran-Contra Affair*  
*PFIAB (President's Foreign Intelligence Advisory Board)*  
*President of the United States (Executive Command and Control of Intelligence Agencies)*

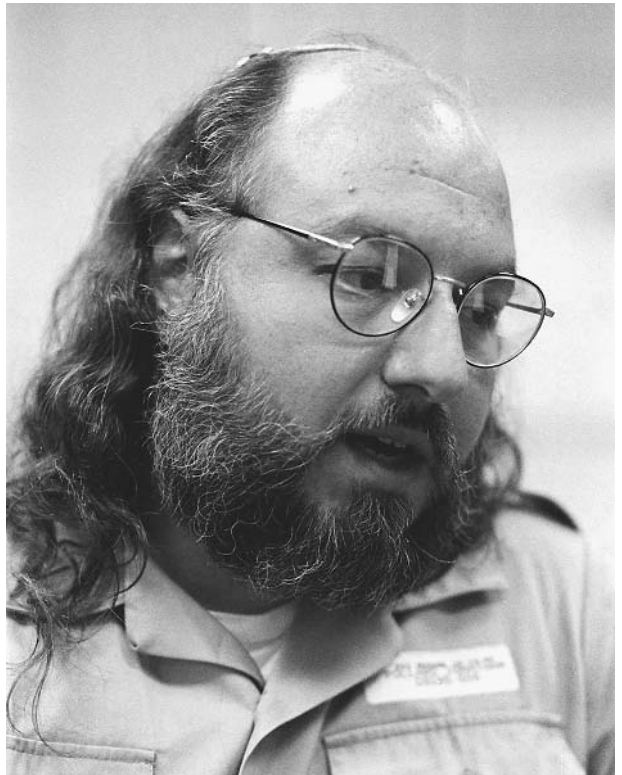
## Pollard Espionage Case

Jonathan Jay Pollard, a veteran of U.S. Navy intelligence forces, sold secrets to the Israeli government during the 1980s. Pollard fed Israel intelligence information regarding Israeli rivals in the Middle East and beyond. Pollard claimed that although he did spy for Israel, he did not conduct espionage against the United States, as the two nations are allies. Following his arrest, Pollard's case drew international attention.

Born in 1954, Pollard was instilled with a devotion to Israel at an early age. He majored in political science at Stanford University. Pollard's questionable activities began there, when he falsely told classmates he had dual citizenship in the United States and Israel, and that he was a member of the Mossad, an Israeli secret agency. He longed to emigrate to Israel, imagining himself as a fantastic character of espionage, fighting on Israel's behalf. Instead of moving to Israel, however, he went to Boston and enrolled in a graduate program at Fletcher School of Law and Diplomacy at Tufts University. At Tufts, he provided information on foreign students to the CIA.

Although he already had his foot in the door with the CIA, the agency turned him down when he applied for a job. In 1979, he gained employment with U.S. Naval Intelligence as a civilian intelligence analyst. Working in Washington, Pollard quickly became disillusioned with what he viewed as an anti-Semitic attitude among his co-workers. After attending a 1982 meeting between U.S. Navy and Israeli intelligence officers, Pollard was convinced that Israeli security was threatened because the U.S. was withholding crucial secrets from its ally.

When a friend called to tell Pollard he had met Colonel Aviem Sella, a noted Israeli war hero, Pollard insisted the friend set up a meeting between himself and Sella. Pollard was initially screened by Israeli intelligence, and Sella was cleared by his superiors to meet confidentially with Pollard at the coffee shop of the Washington Hilton Hotel on May 29, 1984. Pollard told Sella his goal was to supply Israel with U.S. secrets to help the country "strengthen its defense capability." The next time the two met, Pollard handed over 48 documents, and the relationship was secured.



Jonathan Pollard, a former U.S. Naval Intelligence clerk, grants an interview at the Federal Correction Institution in Butner, NC, where he is serving a life sentence for passing military secrets to Israel. AP/WIDE WORLD PHOTOS.

Because of his high-level security clearance, Pollard had the authority to check out classified documents and take them home. Israel became hungry for the information, and Pollard was soon smuggling out suitcases full of classified material. The U.S. government claimed Pollard leaked classified information on the Pakistani nuclear-bomb program, Iraqi and Syrian chemical weapons, Libyan air defenses, and the layout of the Palestine Liberation Organization's headquarters in Tunisia, which Israel then bombed. All told, he photocopied and turned over more than 1,000 classified messages and 800 documents to Israel. In exchange for the information, the Israeli government paid Pollard \$2,500 per month, in addition to trips to Europe and a \$7,000 ring for his wife, who reportedly knew of his espionage activities.

The Federal Bureau of Investigation (FBI) was finally alerted to the quantities of files that Pollard was signing out, but Pollard portrayed himself as a dedicated researcher, working even at home. The FBI did not act immediately, but shadowed Pollard around the clock, suspecting that he might meet with a foreign representative, and give the FBI insight into what he was doing with the material.

In 1985, fearing the increased suspicion of FBI investigators, Pollard and his wife decided to seek asylum and flee to Israel. The two drove to the Israeli Embassy in



Washington, D.C., tailgating a diplomatic limousine through the embassy's front gates. Pollard requested political asylum using his own name, and Danny Cohen, the pseudonym he had been given by the Israeli government, but to no avail. Once turned out by embassy guards, the two were picked up by the FBI.

Pollard was charged with espionage and sentenced to life in prison. According to his supporters, Pollard was the only person in history to spy for an ally and receive a sentence longer than ten years. His wife was charged with collusion and was sentenced to five years in prison.

Although the Israeli government initially denied any involvement with Pollard, they later granted him citizenship. His potential release to return to Israel became a hot-button item. Israel threatened to cease peace talks with the U.S. until the issue was resolved, but failed to gain Pollard's release from prison. Pollard's case was considered by Presidents Reagan, Bush, and Clinton, all of whom denied him clemency.

#### ■ FURTHER READING :

##### BOOKS:

Nash, Jay Robert. *Spies: A Narrative Encyclopedia of Dirty Deeds and Double Dealing from Biblical Times to Today*. N.p., M. Evans, 1997.

##### SEE ALSO

*CIA (United States Central Intelligence Agency) Israel, Intelligence and security*

---

## Polygraphs

---

#### ■ JULI BERWALD

A polygraph test is administered to determine whether or not statements made by the subject taking the test are deceptive. During the test, the subject is monitored by a polygraph machine and interrogated by an administrator trained in forensic psychophysiology. The machine measures changes in the subject's blood pressure, heart rate, respiration rate and sweat production. The theory underlying the polygraph test is that a person who is lying exhibits involuntary physiological responses that can be detected by the polygraph instrument. These changes include rapid breathing and heartbeat and increased blood pressure and perspiration.

### The Polygraph Instrument

The polygraph instrument usually measures four to six physiological reactions recorded by three different medical instruments that are combined in one machine. Older

polygraph machines were equipped with long strips of paper that moved slowly beneath pens that recorded the various physiological responses. Newer equipment uses transducers to convert the information to digital signals that can be stored on computers and analyzed using sophisticated mathematical algorithms.

The three components of the polygraph instrument include the cardio-sphygmograph, the pneumograph, and the galvanograph. Blood pressure and heart rate are measured by the cardio-sphygmograph component of the polygraph, which consists of a blood pressure cuff that is wrapped around the subject's arm. During the questioning the cuff remains inflated. The movement of blood through the subject's veins generates a sound that is transmitted through the air in the cuff to a bellows that amplifies the sound. The magnitude of the sound relates to the blood pressure and the frequency of the changes in the sound relates to the heart rate. The pneumograph component of the polygraph records the subject's respiratory rate. One tube is placed around the subject's chest and a second is placed around his or her abdomen. These tubes are filled with air. When the subject breathes, changes in the air pressure in the tubes are recorded on the polygraph. The galvanograph section records the amount of perspiration produced. It consists of electrical sensors called galvanometers that are attached to the subject's fingertips. The skin of the fingertips contains a high density of sweat glands, making them a good location to measure perspiration. As the amount of sweat touching the galvanometers increases, the resistance of the electrical current measured decreases and these changes are recorded by the polygraph. Most forensic psychophysicologists (FPs) consider the cardio-sphygmograph and the pneumograph components more informative than the galvanograph.

### The Polygraph Test

During the polygraph test, the examiner and the subject are alone in the questioning room. Before the test begins, the examiner spends about an hour talking with the subject. Most forensic psychophysicologists consider this pre-test phase an extremely important part of the polygraph. The examiner obtains a baseline read on his or her emotional state and develops the questions that are asked during the actual test. Before the test begins, the examiner goes over each question with the subject so that he or she knows exactly what to expect. When they are ready start, the person administering the polygraph attaches the various components of the polygraph instrument to the examinee.

The polygraph test itself usually consists of about 10 to 12 questions that require yes or no responses. Several methods of composing questions for polygraph tests exist, but all include asking the subject both relevant questions and control questions. Relevant questions relate



New recruits at the FBI Academy must undergo lie detector tests. ©ANNA CLOPET/CORBIS.

directly to the focus of the polygraph test. Examples of relevant questions are “Did you commit crime X?” or “Did you ever use drug Y?” Control questions vary depending on the type of test administered. The most common type of polygraph test is the Control Question Test (CQT), in which control questions are composed so that the subject can answer them honestly, however, the examiner may make them slightly provocative to evoke an emotional response. Examples of control questions are “Did you ever think of doing crime Y?” or “Were you ever drunk in the last year?” This allows the examiner to understand the subject’s physiological responses to challenging questions. In the CQT, greater physiological responses to the relevant questions than to the control questions indicate deceptive behavior.

There are variations to the CQT. In Directed Lie Tests (DLT), the examiner substitutes very broad questions for the control questions and the subject is directed to answer them with lies. An example is “Have you ever told a lie?” to which the subject is directed to respond “No.” This response gives an examiner an understanding of the subject’s physiological response associated with lying. In Positive Control Tests (PCT), a relevant question itself is used as a control. The subject is instructed to answer truthfully the first time the question is asked and falsely the second time it is asked. The only factor that influences

the response is whether or not the subject is lying. In the Truth Control Test (TCT), the control questions are composed to make the subject think that he or she is being accused of a fictitious crime. This gives the examiner information on how the subject responds to a truthful denial.

During the post-test, the forensic psychophysicist analyzes the subject’s responses to the questions and scores them. Each channel of the polygraph is scored individually. For any channel, if the control response is larger than the relevant response, the score is from +1 to +3, depending on the magnitude of the difference. If the relevant response is larger the score is from –1 to –3. The scores are summed over all channels and all repetitions of the questions to get to the total score. If the final score is sufficiently large and positive, then the subject is considered to have made truthful statements. If the final score is sufficiently large and negative, then the statements are considered deceptive. If the result is close to zero, then the test is inconclusive.

There is much debate as to the accuracy of polygraph tests. Most forensic psychophysicists agree that the rate of detecting deceptive behavior is greater than the rate of detecting truthful behavior. The American Polygraph Association claims that the accuracy rate for polygraph tests is between 85 and 95 percent. However, reports of false positives have reached as high as 75 percent

in research done by the Congressional Office of Technology Assessment.

## History and Uses of the Polygraph

Methods for determining whether or not a person is lying have been part of civilization since ancient times. Ancient Hindus required an accused person to chew a mouthful of rice and then spit it out on a leaf from a sacred tree. If the person could spit the rice he or she was declared honest and if the rice stuck in the mouth, dishonest. This test presumptively relies on the physiological response, which makes a person's mouth dry when being deceptive. In the nineteenth century, Italian criminologist Cesare Lombroso developed an early device for measuring and determining the pulse and blood pressure of a person undergoing interrogation, similar to the cardio-sphygmograph component of the polygraph. In the early 1900s, Russian psychologist A. R. Luria measured the reaction time and tremors in the fingers of suspected criminals.

A student in experimental psychology at Harvard University, William M. Marston invented the modern polygraph prior to 1921. His treatise *The Lie Detector Test* on understanding physiological responses related to deception was published in 1938. John A. Larson, a police officer in Berkeley, California, modified Marston's polygraph, developing a technique for continuous recording of physiological responses. One of Larson's colleagues, Leonard Keeler, added the galvanograph component to the polygraph. He joined the faculty of Northwestern University School of Law in Chicago in 1930 and established the Keeler Polygraph Institute of Chicago.

Lawyer, John E. Reid played an important role in the development of questioning techniques used during a polygraph test. In a 1947 paper, he described the use of control questions to evoke emotional responses. In collaboration with Cleve Backster's work, this idea eventually became the Control Question Test (CQT), which is used by the majority of forensic psychophysicists today.

During the 1960s and 1970s, the polygraph business grew rapidly. Employee screening became a multi-million dollar industry. Polygraph testing began to be used routinely in police work and polygraphers were used as expert witnesses in criminal court trials.

During the late 1970s and early 1980s, the use of the polygraph by the military and security agencies expanded drastically. Between 1973 and 1983, polygraph tests by the federal government tripled. By 1985, the Department of Defense was administering 25,000 tests a year. They used polygraphs to screen employees for classified status, for counterintelligence and for criminal investigations. The FBI, CIA, and National Security Agency used the polygraph to screen job candidates. In 1979, two-thirds of the people rejected for employment from CIA jobs were rejected on the basis of failed polygraph tests.

In the 1980s the scientific validity of polygraphs was brought into question by psychologists. In 1988, the federal Polygraph Protection Act was passed, prohibiting employers from using polygraphs for employment screening. As a result of this legislation, businesses can ask an employee to take a polygraph, but the employee's refusal will not result in any disciplinary treatment. This law does not protect government employees, including people who work in schools, prisons, public agencies, and businesses under contract with the federal government.

The use of polygraphs in court was brought to trial in 1989. In the case of *United States v. Piccinonna*, a polygraph was deemed admissible as evidence, only if both sides agree to its use or the judge allows it based on criteria set forth in the case. A Supreme Court ruling in 1998 expanded the judge's authority in the use of polygraphs in federal cases. Some states accept this ruling, but not all. On the state level, polygraph use is dependent upon the judge and the case. And, in *U.S. v. Schellee* (1998), the Supreme Court upheld a personal evidentiary rule against the admissibility of polygraph evidence at military trials.

### ■ FURTHER READING:

#### BOOKS:

- Harrelson, Leonard. *Lietest: Deception, Truth and the Polygraph*. Ft. Wayne, IN: Jonas Publishing, 1998.
- Lykken, David T. *A Tremor in the Blood: Uses and Abuses of the Lie Detector*. Reading, MA: Perseus Books, 1998.
- Jussim, Daniel. *Drug Tests and Polygraphs*. New York: Julian Messner, 1987.

#### ELECTRONIC:

- How Stuff Works. "How Lie Detectors Work." <<http://science.howstuffworks.com/lie-detector.htm/printable>> (April 15, 2003).
- American Polygraph Association. <<http://www.polygraph.org/>> (April 15, 2003).

---

## Polymerase Chain Reaction (PCR)

---

### ■ BRYAN R. COBB

The Polymerase Chain Reaction, or PCR, refers to a widely used technique in molecular biology that has become quintessential in many aspects of DNA analysis with broad-based applications in medicine and forensic investigations. PCR is the amplification of specific sequences of genomic DNA, the genetic material found in virtually all living cells. This technology was conceived by the Californian geneticist Kary B. Mullis (1944), who won a Nobel Prize in chemistry in 1993 for developing PCR. It was



A scientist at the U.S. Army's biodefense laboratory at Ft. Detrick, Maryland, performs PCR analysis on anthrax samples. AP/WIDE WORLD PHOTOS.

first applied to basic science research and later revolutionized modern medicine by improving the diagnosis of human diseases through enhanced genetic testing and medical research. More recently, PCR technology has significantly contributed to both domestic and international forensic sciences as well as applications aimed at improving United States homeland security.

PCR requires specialized equipment that is customized to fluctuate between specifically timed temperature variations. Before PCR is performed, DNA must be isolated from peripheral blood, hair follicles, cheek cells, or tissue samples. Isolated DNA is double stranded, meaning that there are two sequences of letters or nucleotide bases (A or adenine, G or guanine, C or cytosine, and T or thymine). The double stranded DNA is held together by complementary base pairings in that A binds to T, C binds to G and vice versa. Therefore, knowing of the sequence of one strand will reveal the sequence of the complementary strand. Amplification is necessary because there are 3.9 billion bases, and although there is a lot of total DNA, there is not enough to properly analyze specific gene or gene segments. Amplification, therefore, makes it possible to

obtain ample quantities of specific sequences of DNA to perform a variety of analyses.

PCR requires "primers," or two sequences about 20–25 bases long with one binding to the beginning sequence of interest and the other binding at the end of the same sequence. In order to get the primers to bind to the targeted sequences in the genome, the PCR machines will undergo several cycles at different temperatures. In the first cycle, the DNA is heated to break apart the two strands. The temperature is then reduced so that the primers can bind or anneal to their complementary base sequence in the DNA. Finally, an enzyme called Taq polymerase adds letters from a pool of bases or letters included in the reaction to the position next to the last base of each the primer. Synthesis of one strand of DNA is in the opposite direction of the other. The result is a double stranded DNA sequence. These cycles are repeated several times and amplification of first the DNA sequence in the genome is copied and this copied DNA is re-copied in the next cycle resulting in exponential growth of the specific sequence. Thirty cycles amplified the target DNA between 100,000- to 10,000,000-fold. However, only DNA

sequences of 100 to 2000 bases long are ideally suitable for PCR amplification. In this way, a gene of interest or part of the gene can be amplified to quantities that make genetic studies possible.

PCR, therefore, is rapid, inexpensive, and a relatively easy way of producing a large number of copies of a specific DNA sequence. This is particularly advantageous when there is very little or poor quality DNA. RNA, which is converted from DNA into protein, can also be amplified in the same manner as DNA, however, DNA is much more stable and is easier to isolate. Since each individual inherits sequences of DNA that are different from other individuals, the importance of DNA and PCR technology in identifying an individual is exemplified in the courtroom. DNA analysis can be a powerful tool in criminal investigations, especially those classified as homicides, theft, and sexual assault. Physical evidence left at the scene of any crime can be helpful in reconstructing the sequence of events and potentially reveal the criminal. It can also reveal non-paternity if the pattern of DNA in the offspring does not match the pattern of DNA in the assumed father.

Forensic science relies heavily on PCR technology to amplify specific sequences of DNA that will establish a connection between a specific suspect and a crime scene. Amplification of DNA is critical in cases where the source of DNA is minimal or the integrity is compromised. DNA evidence is also a powerful tool that has been used to ultimately prove the innocence of previously convicted individuals. Additionally, DNA can reveal many characteristics that can help forensic scientists and law enforcement officers identify the perpetrator. This is becoming increasingly applicable to national security as well as international intelligence. PCR has revolutionized law enforcement in this way and will continue to enhance the justice system in the future. For example, using complex algorithms and known sequences of DNA, it is possible to analyze the genetic DNA pattern from an unknown person to predict eye color, gender, and even ethnicity.

In 1985 American geneticist Alec Jeffreys, Ph.D. used PCR technology to amplify regions in the human genome that were highly variable. These DNA fragments were comprised of specific sequences that were repeated. The repeat number was found to be highly variable from individual to individual with the exception of identical twins. These DNA fragments could be amplified using PCR and then studied for variable fragment lengths of repeats. This technology was collectively referred as genetic fingerprinting and became widely used. In a highly publicized case called the Narborough Murder Enquiry, criminal investigators were able to identify the perpetrator using DNA fingerprinting.

One of the more recent applications of PCR technology is for improving national security. After the September 11, 2001 terrorist attacks on the United States, the fear of further attacks involving biological weapons increased. Rapid identification of terrorists and specific biological agents using PCR-based methods represents a plausible

approach to gathering critical information about these individuals and weapons.

With the identification, characterization, and genetic engineering of viruses, bacteria, and fungi, the likelihood of strategic, harmful applications involving these organisms is growing. Biological species that represent a serious health risk to humans have been used as weapons for years. These risks can include the U.S. agricultural economy, food supplies, and the environment. To combat bioterrorism, President George W. Bush in February 2002 called for a budget increase to \$5.9 billion for Homeland Security directed towards protecting against bioterrorist attacks. The creation of a national database that catalogs pathogens and individuals that are authorized to study these pathogens is also of ongoing concern. A benefit of these databases would be to identify the genetically engineered pathogens used as biological weapons (allowing quick access to specific medical treatment protocols) and to potentially link pathogens to the bioterrorists that developed them.

PCR technology can also be employed to identify the specific disease-causing microorganism. The U.S. Postal Service is working in conjunction with the biotech industry on initiatives to develop intelligent mail. Using PCR to identify anthrax, for example, is one way to quickly ascertain the nature of the contaminated mail or screen high-risk mail. This technology was the government's primary weapon against mail deemed unsuitable for circulation since irradiation provided a limited, unsubstantial solution and often damaged the mail. This high-tech strategy for mail surveillance can be particularly useful by sucking out air samples from the mail and testing for specific molecular signatures using PCR to detect a possible biological contaminant.

Defending against bioterrorism after the September 11 attacks includes developing advances in biological detection instrumentation. In conjunction with the Centers for Disease Control and Prevention (CDC), Lawrence Livermore National Laboratory and its sister laboratory at Los Alamos are currently developing DNA profiles of the most threatening pathogens such as anthrax and the plague using PCR technology. Biodetection instrumentation for genetic profiling has led to the miniaturization and subsequently the portability of DNA analytical devices, particularly for PCR. Forensic scientists and criminologists also benefit from mobile PCR machines by bringing the science to the scene of the crime leading to more rapid crime-solving capabilities.

Security at the 2002 Winter Olympic Games in Salt Lake City was led by The Biological Aerosol Sentry and Information System (BASIS). Miniaturized PCR machines called Smart Cyclers developed by a company called Cepheid were used at the field laboratory operation set up by BASIS. The purpose was to prepare for a bioterrorism threat by having appropriate and rapid biological sample identification to allow for accurate bioterrorist assessment and validation so that the proper responses could be executed.

Recent concerns over genetic engineering of agricultural food products and the potential risks to food safety have prompted studies investigating the molecular signatures of crops using PCR. A study in the scientific journal *Nature* revealed that genetically manipulated DNA from industrial produced maize had been introduced into corn fields in Oaxaca, Mexico. Although the ramifications to health and food safety are unknown and most likely benign, surveillance of crops using PCR is a formidable approach in the implementation of security measures to help protect against harmful pathogenic contaminations that can threaten food safety. As the cost and use of PCR are eased and as the collection of databases with recognizable DNA profiles of various microorganisms is increased, the utility of this technology in human and food safety will be greatly improved.

■ FURTHER READING:

BOOKS:

Friedman, J., F. Dill, M. Hayden, and B. McGillivray. *Genetics*. N.P.: Williams & Wilkins, 1996.

Lodish, J., D. Baltimore, A. Berk, S. L. Zipursky, P. Matsudaira, and J. Darnell. *Molecular Cell Biology*. New York: Scientific American Books, 1995.

PERIODICALS:

Jeffereys, A. J. "Hypervariable 'minisatellite' regions in human DNA." *Nature* no. 314 (1987): 67–73.

Mullis, K. B., and F. A. Faloon. "Specific synthesis of DNA in vitro via a polymerase catalysed chain reaction." *Methods in Enzymology* no. 155 (1987): 335–350.

Nakamura, Y., M. Leppert, P. O'Connell, et al. "Variable number tandem repeat (VNTR) markers for human gene mapping." *Science* no. 237 (1987): 1616–1622.

Quist, D., and I. H. Chapela. "Transgenic DNA introgressed into traditional maize landraces in Oaxaca, Mexico." *Nature* no. 414 (2001): 541–3.

Wong, Z., V. Wilson, A. J. Jeffereys, et al. "Cloning a selected fragment from a human DNA 'fingerprint': isolation of an extremely polymorphic minisatellite." *Nucleic Acids* no. 14 (1986): 4605–616.

Wyman, A. R. and R. White. "A highly polymorphic locus in human DNA." *PNAS* no. 77 (1980): 6754–6758.

ELECTRONIC:

Access Excellence. "Kary B. Mullins." The National Health Museum. March, 2002. <[http://www.accessexcellence.org/AB/BC/Kary\\_B\\_Mullins.html](http://www.accessexcellence.org/AB/BC/Kary_B_Mullins.html)> (December 13, 2002).

Access Excellence. "PCR Technology." Connie Veilleax. July 8, 2002. <[http://www.accessexcellence.org/LC/SS/PS/PCR/PCR\\_technology.html](http://www.accessexcellence.org/LC/SS/PS/PCR/PCR_technology.html)> (December 16, 2002).

Center for strategic and international solutions. "New Technology Counters Bioterrorism Threat, Policy Issues." CSIS. Fall, 2002. <[http://www.csis.org/pubs/prospectus/02fall\\_bacastow.htm](http://www.csis.org/pubs/prospectus/02fall_bacastow.htm)> (December 11, 2002).

Edvotek. "Biotechnology: DNA Fingerprinting for Forensics and Paternity." 2001. <<http://www.edvotek.com/experiments/biotech/04/334.html>> (December 12, 2002).

Government Security. "Who are you?" Technology solutions in defense of the homeland. July 22, 2002. <<http://govtsecurity.securitysolutions.com>> (December 15, 2002).

Kari Sable Burns. "Green River Killer." True Crimes. 2002. <<http://www.karisable.com/greenriverdnatime.htm>> (December 15, 2002).

United States Congress 107th Congress 2nd Session. "Technology assessment in the war on terrorism and homeland security: the role of OTA" Committee Print. April, 2002. <[http://www.fas.org/irp/congress/2002\\_hr/ota.html](http://www.fas.org/irp/congress/2002_hr/ota.html)> (December 15, 2002).

Westburg. "Human Diagnostics: forensics." Cambridge Molecular Diagnostics. 2001. <[http://www.westburg.nl/html/md/hd\\_forensics.htm](http://www.westburg.nl/html/md/hd_forensics.htm)> (December 15, 2002).

SEE ALSO

*Anthrax*

*Anthrax, Terrorist Use as a Biological Weapon*

*Anthrax Vaccine*

*Anthrax Weaponization*

*Biochemical Assassination Weapons*

*Biocontainment Laboratories*

*Biodetectors*

*Bio-Engineered Tissue Constructs*

*Biological and Toxin Weapons Convention*

*Biological Warfare*

*Biological Warfare, Advanced Diagnostics*

*Biological Weapons, Genetic Identification*

*CDC (United States Centers for Disease Control and Prevention)*

*Chemical and Biological Defense Information Analysis Center (CBIAC)*

*Microbiology: Applications to Espionage, Intelligence and Security*

*Microchip*

---

## Popular Front for the Liberation of Palestine (PFLP)

---

At one time affiliated with the PLO, the Popular Front for the Liberation of Palestine (PFLP) is a Marxist-Leninist group founded in 1967 by George Habash. The PFLP joined the Alliance of Palestinian Forces (APF) to oppose the Declaration of Principles signed in 1993 and suspended participation in the PLO. The PFLP broke away from the APF, along with the DFLP, in 1996 over ideological differences. PFLP officers took part in meetings with Arafat's Fatah party and PLO representatives in 1999 to discuss national unity and the reinvigoration of the PLO but the PFLP continues to oppose current negotiations with Israel.

PFLP committed numerous international terrorist attacks during the 1970s. Since 1978, PFLP has conducted attacks against Israeli or moderate Arab targets, including

killing a settler and her son in December 1996. The PFLP increased operational activity in 2001, highlighted by the shooting death of the Israeli tourism minister in alleged retaliation for Israel's killing of a PFLP leader.

The PFLP is estimated to have approximately 800 members, and has operated in Syria, Lebanon, Israel, West Bank, and Gaza. They receive safe haven and logistical assistance from Syria.

#### ■ FURTHER READING :

##### ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001. Annual Report: On the Record Briefing. May 21, 2002. <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

##### SEE ALSO

*Terrorism, Philosophical and Ideological Origins Terrorist and Para-State Organizations Terrorist Organization List, United States Terrorist Organizations, Freezing of Assets*

---

## Popular Front for the Liberation of Palestine-General Command (PFLP-GC)

---

The Popular Front for the Liberation of Palestine-General Command (PFLP-GC) split from the Popular Front for the Liberation of Palestine (PFLP) in 1968, claiming it wanted to focus more on fighting and less on politics. Opposed to Arafat's Palestine Liberation Army (PLO), the PFLP-GC is led by Ahmad Jabril, a former captain in the Syrian Army. The PFLP-GC maintains close ties to both Syria and Iran.

The PFLP-GC carried out dozens of attacks in Europe and the Middle East during the 1970s-80s. Known for cross-border terrorist attacks into Israel using unusual means, such as hot-air balloons and motorized hang gliders, PFLP-GC's recent primary focus is on guerrilla operations in southern Lebanon, small-scale attacks in Israel, West Bank, and Gaza.

The PFLP-GC has an estimated several hundred adherents, and is headquartered in Damascus with bases in Lebanon. They receive support from Syria and financial support from Iran.

#### ■ FURTHER READING :

##### ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001. Annual Report: On the Record Briefing. May 21, 2002. <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

##### SEE ALSO

*Terrorism, Philosophical and Ideological Origins Terrorist and Para-State Organizations Terrorist Organization List, United States Terrorist Organizations, Freezing of Assets*

---

## Port Security

---

Security of national ports has always been a concern for any great power, but between the War of 1812 and the terrorist attacks of September 11, 2001, Americans tended to take such security for granted. Other than a thwarted German attempt to form an alliance with Mexico against the United States—an effort that brought America into World War I—and limited Axis attempts to infiltrate both coasts in World War II, no foreign power launched a successful attack on the contiguous United States prior to the al Qaeda bombings. Since September, 2001, the federal government has adopted much stricter standards for port security. Key elements in this undertaking are the U.S. Coast Guard (USCG), the U.S. Customs Service, and the two agencies' parent organization, the Department of Homeland Security.

On September 24, 2001, less than two weeks after the terrorist attacks on the World Trade Center in New York, the House Transportation and Infrastructure Committee and the Senate Commerce, Science, and Transportation Committee issued a joint request to Transportation Secretary Norman Mineta for a rapid response team to reduce the vulnerability of American ports to terrorist attack. In accordance with this request, Mineta requested additional funds for his department's leading antiterrorism service, the USCG.

At that time, several statutes already existed providing USCG with extensive enforcement powers. These included Section 89 of Title 14, U.S. Code, which authorized USCG to board any vessel subject to the jurisdiction, or operation of any law, of the United States in order to make inquiries or conduct examinations, inspections, searches, seizures, or arrests. The Ports and Waterway

Safety Act of 1972 gave the Secretary of Transportation broad authority to regulate movements and activities of vessels subject to U.S. jurisdiction, with USCG as Transportation's operational arm in these undertakings.

Additional powers came from the Omnibus Diplomatic Security and Antiterrorism Act of 1986, passed after a U.S. citizen was killed during the terrorist seizure of the passenger vessel *Achille Lauro* in 1985. Title XI of that law became known as the International Maritime and Port Security Act. The latter gave USCG authority to require inspections, patrol ports and harbors, establish security and safety zones, and develop contingency plans and procedures in an effort to combat terrorism.

## USCG Responds to 9/11

As Mineta noted before the joint committees, USCG had launched "the largest homeland port security operation since World War II" in the aftermath of September 11. As part of Operation Noble Eagle and Enduring Freedom, first phases of the effort to destroy al Qaeda, USCG deployed 55 cutters (small armed vessels), 42 aircraft, and hundreds of boats to establish port and coastline patrols. It also called up more than 2,800 reservists to support homeland security operations at the country's 361 ports.

At the ports of San Francisco, Los Angeles, and San Diego, USCG developed a pilot armed escort initiative, the Sea Marshals program, whereby it provided armed escort to vessels during their transit through U.S. waters. USCG also established Naval Vessel Protection Zones, the maritime equivalent of no-fly zones, for a distance of 500 yards (457 m) around all U.S. naval vessels in the navigable waters of the United States.

Vital to these operations, and to future efforts to protect U.S. ports, were USCG Port Security Units (PSUs). Staffed primarily with selected reservists, along with a core of active duty personnel, PSUs had a mission of providing waterborne security, along with limited land-based protection, for shipping and critical port facilities both in U.S. waters and in theatres of combat. In the latter capacity, PSUs had been deployed to the Persian Gulf during Operation Desert Storm in 1990, and to Haiti for Operation Uphold Democracy in 1994. In December, 2000, following the terrorist attacks on the USS *Cole* in Yemen, PSU 309 from Port Clinton, Ohio, was deployed to the Middle East to provide vital force protection for Navy assets.

Capable of deploying within 24 hours and establishing operations within 96 hours after initial call-up, PSUs had transportable boats equipped with dual outboard motors, along with support equipment to sustain activities for up to 30 days. Because the specialized training for PSU operations was not available within USCG, reservists assigned to PSUs were required to undergo a two-week basic skills course at the PSU Training Detachment, located on the U.S. Marine base at Camp Lejeune, North Carolina.

## The Maritime Security Act

On November 15, 2002, the House passed the Maritime Security Act, approved by the Senate two days earlier. Among other provisions, the new legislation extended USCG powers by giving its units authority to require background checks of some port employees; put in place a new tracking system for commercial ships; require all 361 nationwide ports to establish committees bringing together federal, state, local, and private security officers; establish marine anti-terrorism methods; set new standards to make container seals tamper-proof; and authorize the Sea Marshal program.

Congress appropriated \$500 million to dispatch more security operatives to inspect cargo at its point of origin, and for other specific measures that included development of equipment to detect nuclear, biological, and chemical weapons hidden in containers. In securing the nation's 25,000 miles of navigable waterways, USCG called on the help of TRW Systems, to which it awarded a \$31-million, five-year contract to assess security measures and assist in developing guidelines, as well as self-assessment methodology.

An example of new container security measures could be found at the busy port of Hampton Roads, Virginia, where U.S. Customs had installed radiation detection equipment to interdict hidden radioactive material. Hampton Roads authorities reported that the alarm sounded two or three times a week, each time for reasons that had nothing to do with terrorism: smoke detectors, for instance, have trace amounts of radioactive materials, as do some medications and plants. These false alarms caused only minor delays, and port security officials gave the \$125,000 system high marks.

Likewise, maritime industry representatives attending a public hearing sponsored by USCG in San Pedro, California, in February, 2003, expressed approval of new plans for increased security in the local port. However, they did request federal assistance in raising the estimated \$6 billion needed to put the new measures in place.

Funding issues were also a concern for Senator Ernest Hollings (D-SC), former chairman of the Senate Commerce Committee and sponsor of the Maritime Security Act. He had hoped to raise several hundred million more dollars through users' fees on cargo and shipping companies, a move bitterly opposed by the shipping industry. Due to this opposition, Hollings had removed the fee from his original bill, but in March, 2003, his staffers told the *Chicago Tribune* that he intended to keep pursuing the idea.

**Continuing concerns.** A number of situations in late 2002 and early 2003 highlighted the need for increased port security measures. One of these was a war game staged in the fall of 2002 by some 85 officials representing the Central Intelligence Agency, Federal Bureau of Investigation, Office of Homeland Security (as the new department was called prior to March 2003), and international trade businesses.



The premise was a terrorist plot to deliver weapons of mass destruction to the United States through one of its ports. In order to stop the attack, participants searched ports nationwide, yet they failed to find the “terrorists,” who succeeded in smuggling their deadly cargo in a container through a port on the East Coast. Had these been real terrorists, they would have been free to explode a “dirty bomb” (radioactive material packed with explosives) in the middle of downtown Chicago, their target in the exercise.

A contract dispute between dock workers and employers on the West Coast in the fall of 2002 shut down ports for 10 days, causing a \$1 billion impact on retailers—thus, illustrating the devastating economic impact a shut-down could have. Participants in the war games exercise calculated that, if U.S. ports had to shut down because of a terrorist incident, the Dow Jones industrial index could rapidly plunge and leave a dent in the economy measured in the tens of millions within a day.

Other real-life incidents and phenomena raised concerns during this period. A boatload of illegal immigrants from Haiti penetrated port security in Miami in early 2003, and periodically stowaways from China managed to get into the ports of the West Coast inside shipping containers. Far more ominous were reports throughout 2002 of al Qaeda “ships of concern,” with U.S. intelligence estimating that the terrorist group had anywhere from 12 to 50 rogue vessels plying the world’s seas.

#### ■ FURTHER READING :

##### PERIODICALS:

Brand, Lois. “Helping Coast Guard Enhance Port Security.” *National Defense* 87, no. 590 (January 2003): 45.

Haynes, V. Dion. “U.S. Works to Shore up Port Security; War Game Underscores Acute Risk.” *Chicago Tribune*. (March 10, 2003): 8.

Mintz, John. “15 Freighters Believed to Be Linked to al Qaeda.” *Washington Post*. (December 31, 2002): A1.

Schoch, Deborah. “Port Security Upgrade Welcomed, But Industry Asks Who Will Pay.” *Los Angeles Times*. (February 6, 2003): B3.

##### ELECTRONIC:

Meeks, Brock N. Container, Port Security Seen Lacking. MSNBC News. <<http://www.msnbc.com/news/888290.asp?0s=>>> (March 29, 2003).

Port Security Units. U.S. Coast Guard. <<http://www.uscg.mil/hq/g-cp/comrel/factfile/Factcards/PSUs.html>> (March 29, 2003).

The Subcommittee on Coast Guard and Maritime Transportation Hearing on Port Security. House of Representatives. December 6, 2001. <<http://www.house.gov/transportation/cgmt/12-06-01/12-06-01memo.html>> (March 29, 2003).

##### SEE ALSO

*Coast Guard (USCG), United States*

*Customs Service, United States*  
*Homeland Security, United States Department of*  
*September 11 Terrorist Attacks on the United States*

## PORTPASS (Port Passenger Accelerated Service System)

PORTPASS (Port Passenger Accelerated Service System) is a generic term for programs developed to expedite passage through U.S. national entry systems. PORTPASS components include the INSPASS (Immigration and Naturalization Service Passenger Accelerated Service System), SENTRI (Secure Electronic Network for Travelers’ Rapid Inspection), OARS (Outlying Area Reporting Station), and RVIS (Remote Video Inspection System) systems. The general goal of PORTPASS programs is to identify pre-approved low-risk international travelers and allow inspectors additional time to focus on high-risk entrants.

As with other automated entry systems, PORTPASS databases utilize a “one-to-one” search protocol to verify identity. Instead of comparing gathered biometrics or vehicle identification data across a broad database, an identification number allows direct comparison with the data assigned to a PORTPASS identification number.

INSPASS is used at selected airports to facilitate passage through entry checkpoints. INSPASS systems utilize hand geometry biometrics that include measurements of hand length, thickness and translucency.

SENTRI is used at selected border crossings to facilitate quick passage through entry inspection checkpoints. SENTRI programs screen participants and their vehicles against information already gathered in the program database. SENTRI utilizes digital license plate readers and camera scans that allow inspectors to validate both the identity of the vehicle and the identity of the occupants of the vehicle against digitized photographs of approved participants in the SENTRI database and other law enforcement databases.

OARS was developed as a counterpart to the Canadian Border Boat Landing Program (I-68 program) that allows registered participants facilitated entry to U.S. waters for recreational purposes through a self-reporting system located at fueling docks, boating marinas, and state parks.

RVIS is a PORTPASS program in use along the U.S. border with Canada. Using video surveillance, inspectors can remotely monitor border crossings. Inspectors can verify registered RVIS participants and alert enforcement authorities in the event of an unauthorized border crossing. Automated systems are also backed with a video inspection system so that, if the identification systems fail

to provide a positive match to approved database information, inspectors located offsite can still interview the prospective entrant.

As of March 1, 2003, the newly created United States Department of Homeland Security (DHS) absorbed the former Immigration and Naturalization Service (INS). All INS border patrol agents and investigators—along with agents from the U.S. Customs Service and Transportation Security Administration—were placed under the direction of the DHS Directorate of Border and Transportation Security (BTS). Responsibility for U.S. border security and the enforcement of immigration laws was transferred to BTS.

BTS is also scheduled to incorporate the United States Customs Service (previously part of the Department of Treasury). Former INS immigration service functions are scheduled to be placed under the direction of the DHS Bureau of Citizenship and Immigration Services. Under the reorganization, the INS formally ceases to exist on the date the last of its functions are transferred.

Although the technologies involved in PORTPASS entry security programs remain viable, in an effort to facilitate border security, BTS plans currently envision higher levels of coordination between formerly separate agencies and databases. As of April 2003, the specific coordination and future of PORTPASS programs was uncertain with regard to potential name changes, program administration, and policy changes.

## ■ FURTHER READING:

### ELECTRONIC:

Bureau of Citizenship and Immigration Services. INSPASS. March 1, 2003. <<http://www.immigration.gov/graphics/howdoi/inspassloc.htm>> (April 14, 2003).

Department of Homeland Security. April 2, 2003. <<http://www.dhs.gov/dhspublic/index.jsp>> (April 11, 2003).

Department of Homeland Security. Secure Electronic Network For Travelers Rapid Inspection (SENTRI). March 26, 2003. <<http://www.immigration.gov/graphics/shared/lawenfor/bmgmt/inspect/sentri.htm>> (April 9, 2003).

United States Department of Homeland Security. Bureau of Citizenship and Immigration Services. PORTPASS. March 11, 2003. <<http://www.immigration.gov/graphics/howdoi/portpass.htm>> (April 9, 2003).

United States Department of Homeland Security. Immigration Information. INSPASS. March 4, 2003. <<http://www.immigration.gov/graphics/shared/howdoi/inspass.htm>> (April 9, 2003).

### SEE ALSO

*APIS (Advance Passenger Information System)*

*IBIS (Interagency Border Inspection System)*

*IDENT (Automated Biometric Identification System)*

*INSPASS (Immigration and Naturalization Service Passenger Accelerated Service System)*

*NAILS (National Automated Immigration Lookout System)*

*SENTRI (Secure Electronic Network for Travelers' Rapid Inspection)*

## Portugal, Intelligence and Security

Portugal's tumultuous twentieth-century political history affected public perception of the nation's government and intelligence officials. In the 1940s, António de Oliveira Salazar's dictatorship created a secret police force, the International Police for the Defense of the State (PIDE). The PIDE gained a reputation for domestic and political espionage, and the arrest, detainment, and torture of anti-government dissidents. The secret police operated above the law in Portugal for over three decades, but used especially brutal means of coercion in the nation's African colonies as an attempt to crush independence movements.

After a coup overthrew Salazar's successor, Marcello Caetano, the secret police was abolished. The agency that replaced the PIDE could not overcome the legacy of its predecessor and was quickly dissolved. Public outcry and government apprehension prevented the formation of a new intelligence service in Portugal for over a decade. In the early 1980s, a string of terrorist attacks on Portuguese interests, including the bombing of their embassy in Turkey, prompted the formation of new intelligence and security service. The new Portuguese intelligence service was established by a newly elected progressive government. Constitutional reforms in 1989 guaranteed that the new intelligence services would be regulated by the government and barred from political and domestic espionage.

Today, Portugal maintains both military and civilian intelligence and security forces. The main intelligence agency is the *Sistema de Informacoes da Republica Portuguesa* (SIRP), or the Intelligence System of the Portuguese Republic. The SIRP is charged with the protection of national security by producing and analyzing intelligence information gathered from foreign and domestic sources.

The SIRP is divided into two major operational branches. The Security Information Service (SIS) coordinates military and civilian efforts to protect national military, economic, and government interests. The SIS has both counter-intelligence and anti-terrorism special task forces. While the SIS is controlled by the Ministry of Internal Administration, the Ministry of National Defense operates the other significant SIRP division, the *Serviço de Informações Estratégicas de Defesa e Militares* (SIEDM) or Strategic Defense and Military Intelligence Service. The SIEDM primarily focuses on external intelligence and threats to state property and interests abroad. The agency cooperates closely with the military to conduct defense and anti-terrorism operations.

The Portuguese Armed Forces also maintain their own, individual intelligence units. Operations of all military intelligence forces are classified, but closely monitored by the office of the Prime Minister.

The socialist and democratic socialist parties have continued to vie for power in Portugal's government. Elections held in 2001 yielded a gain of several local offices for the democratic socialists, leading to a turnover in the national government. The current Portuguese government is endeavoring to further the massive constitutional reforms begun in 1986. Portugal is a member of the North Atlantic Treaty Organization (NATO). Part of the European Union (EU), Portugal participates in pan-European intelligence and security organizations as well as the EU currency program.

#### SEE ALSO

*European Union*

---

## Postal Security

---

■ BELINDA ROWLAND

Postal security refers to the safeguarding of United States Postal Service (USPS) employees and customers from hazardous materials that may be contained in the mail.

In October 2001, pieces of mail containing the anthrax bacterium infected 23 persons, five of whom died. The USPS immediately took measures to insure the safety of its employees and customers. Furthermore, the USPS developed a plan to safeguard the mail system and protect employees and customers without compromising the level of mail service.

### USPS Emergency Preparedness Plan

Because of the complexity of the USPS system and volume of mail that is processed, achieving postal security is no small undertaking. The postal service handles nearly 680 million pieces of mail each day. The USPS has about 300 processing and distribution centers that use computer-controlled sorting equipment and data processing systems to distribute mail to its destination.

The Emergency Preparedness Plan was developed to protect USPS employees and customers from future bioterrorism attacks. The Plan is composed of six initiatives: prevention, protection and health-risk reduction, detection and identification, intervention, decontamination, and investigation. Each initiative is a point where actions can be taken to reduce the risk or effects of bioterrorism.

**Prevention.** The first initiative is to reduce the risk that a person could use the mail as a vehicle for bioterrorism.



FBI agents check the identification of a postal worker seeking to enter the Federal Building in Los Angeles as security measures were tightened coast to coast after the terrorist attacks of September 11, 2001. AP/WIDE WORLD PHOTOS.

The addition of detection, containment, and sterilization technologies to the 350,000 mail collection boxes in use is not yet feasible. The USPS has been investigating the use of intelligent mail in which each piece of mail has a unique identifier. This measure would reduce anonymous mail.

**Protection and health-risk reduction.** This initiative's objective is to reduce the risk that USPS employees and customers could be exposed to biological weapons and to prevent contaminated mail from contaminating other mail. USPS employees can wear protective equipment. Mail-processing machinery could be cleaned with high-efficiency particulate air (HEPA)-filtered vacuum systems. Enhanced heating, ventilation, and air-conditioning (HVAC) systems could be used to trap or kill bacteria in the air. As of late 2002, the application of HEPA-filtration technologies to the mail system is still being investigated.

**Detection and identification.** The objective of the third initiative is to detect and identify biological weapons as

early in the mail stream as possible. This initiative involves two technologies: triggering and confirmation. Triggering technologies would provide continuous monitoring of the mail and report the presence of a possible threat. Confirmation technologies would detect the presence of specific microorganisms. Application of these technologies to the mail system is still under investigation.

**Intervention.** Routine decontamination of mail is a precautionary measure. The possible methods for mail decontamination work by exposing mail to radiation (eg. e-beams), high pressure, or gases. Microorganisms, such as the anthrax bacterium or spore, cannot survive these conditions. In 2001, the USPS bought eight e-beam machines and planned to install them in Washington D.C. and the New York and New Jersey area. As of late 2002, irradiation is the only acceptable method for decontaminating mail, and e-beam technology has been used to sterilize incoming federal government mail only.

**Decontamination.** This initiative refers to the elimination of known biological weapons in the mail, mail processing equipment, and buildings. The decontamination processes described for the intervention initiative can be applied to sterilize mail that is known to be contaminated with dangerous microorganisms. Certain gases have antimicrobial properties and are used for disinfection and sterilization. Chlorine dioxide was used to disinfect an office building that was contaminated with anthrax spores.

**Investigation.** This initiative aims to enhance criminal investigation methods as related to postal security. Technologies consistent with this initiative include mailpiece tracking and tracing using a Wide Field of View camera, image capture and analysis, and positive product tracking. These technologies would enable the USPS to track contaminated mail and equipment.

#### ■ FURTHER READING:

##### PERIODICALS:

"Months After Anthrax Scare, Mail-Safety Goals are Unmet." *USA Today*. (August 29, 2002):12a.

Rhodes, Keith A., "USPS Air Filtration Systems Need More Testing and Cost Benefit Analysis Before Implementation." *FDCH Government Account Reports* (August 22, 2002).

##### ELECTRONIC:

United States Postal Service. <<http://www.usps.com/welcome.htm>> (January 1, 2003).

##### SEE ALSO

*Anthrax, Terrorist Use as a Biological Weapon*

*Bioterrorism, Protective Measures  
Decontamination Methods  
Mail Sanitization  
Postal Service (USPS), United States  
September 11 Terrorist Attacks on the United States*

## Postal Service (USPS), United States

The United States Postal Service (USPS) is an independent government agency that collects and disseminates the mail to millions of homes and businesses across the country.

In the early days of America, colonists had to either ferry their own mail or rely on messengers and merchants to carry their letters and packages. The first official postal service emerged in 1639, when Richard Fairbanks' Boston tavern became the repository of all mail sent from abroad. The postal service was initially run by the British, but in 1775, America's Continental Congress voted to establish its own postal system, with Benjamin Franklin as its first postmaster general. By the 1780s, the postal system consisted of seventy-five post offices and about twenty-six post riders. The first postage stamps were introduced in 1847.

Over the next two centuries, the postal service expanded and evolved. Americans' westward expansion gave rise to the Pony Express in the 1860s, a team of horse-riding letter carriers who distributed the mail between Missouri and California. Over the years, letter carriers traded in their horses for faster means of transportation: trains, steamboats, and trucks. With the introduction of the airplane in the early 1900s, the Postal Service could for the first time deliver mail quickly and affordably across the oceans.

The next major overhaul to the postal system occurred on August 12, 1970, when President Richard Nixon signed the Postal Reorganization Act. The Act replaced the old Post Office Department with the U.S. Postal Service. It was designed to make the service run more like a business and less like a government agency. Today, the USPS is directed by an eleven-member Board of Governors, led by a Postmaster General. Postage rates and service fees are decided upon by an independent Postal Rate Commission.

Every day, the USPS handles more than 680 million pieces of mail. The Postal Service relies on the revenue from these deliveries to survive, because it does not receive funding from taxpayer dollars. To protect its customers from mail theft, mail fraud, and other criminal activities involving the mail, the USPS has its own law enforcement agency, called the U.S. Postal Inspection Service. This agency works closely with federal law enforcement officials to ensure that the mail service is safe.

In October 2001, mail security became a matter of national urgency. Following the discovery of anthrax-tainted letters, which ultimately infected twenty-two people and killed five in the northeastern United States, the USPS announced that it was adopting tighter security measures. Many postal facilities were outfitted with state-of-the-art irradiation systems, which sanitize the mail using the same radiation technology that protects the food supply from bacterial contaminants. Also installed were vacuum/filtration cleaning systems to remove hazardous particles from sorting machines.

#### ■ FURTHER READING :

##### BOOKS:

Bolick, Nancy O'Keefe. *Mail Call!: The History of the U.S. Mail Service*. Danbury, CT: Franklin Watts, Incorporated, 1994.

Kule, Elaine A. *The U.S. Mail (Transportation and Communication Series)*. Berkeley Heights, NJ: Enslow Publishers, Inc., 2002.

##### ELECTRONIC:

The United States Postal Service. <<http://www.usps.com/>> (December 20, 2002).

##### SEE ALSO

*Anthrax, Terrorist Use as a Biological Weapon Mail Sanitization Nixon Administration (1969–1974), United States National Security Policy Postal Security*

## Potassium Iodide

Potassium iodide (chemical formula KI) is a salt that is similar in structure and physical character to common table salt (sodium chloride; NaCl). Indeed, potassium iodide is a common commercial additive to table salt, to produce "iodized" salt.

Potassium iodide is noteworthy in security because of its ability to block the uptake of radioactive iodine by the body's thyroid gland. Located in the neck, the sole task of the thyroid gland is the production of a hormone that is one of the body's principle metabolic regulators. Thus, the disruption of the thyroid gland—such as occurs when the uptake of radioactive iodine triggers the development of thyroid cancer—threatens health and can even lead to death.

If taken in time following an accidental or deliberate release of radioactive iodine, such as would occur with a leak from a nuclear power plant or the detonation of a

bomb containing a radioactive payload, potassium iodide saturates the thyroid with a form of iodine that persists in the gland. The radioactive form of iodine cannot out-compete this stable form of iodine, and so is excreted from the body.

Ingestion of KI has long been a precaution for workers in nuclear power plants and for military personnel engaged in a conflict where the use of nuclear weapons is considered to be a possibility. Much of what is known of the protective effects of potassium iodide has come from the measurements of radiation accumulation in the thyroid glands of hundreds of thousands of people in the weeks following the Chernobyl reactor disaster of April 1986, and the therapeutic effects KI achieved in Poland during that time.

Since the terrorist attacks on the United States in the latter months of 2001, the need for a distribution of KI to civilians has become recognized. This has become especially evident with the exposed vulnerability of nuclear power plants to terrorist attack, and to the conceivable use of "dirty" bombs by terrorists. The latter, essentially a conventional explosive charge that spews out radioactive substances including iodine, could contaminate many people in a crowded urban area.

The protective effects of potassium iodide last about 24 hours from the time it is ingested. Thus, a civilian or military protective strategy requires daily doses of KI. Longer term or more permanent use of the salt is not recommended yet, as prolonged use has been linked to thyroid malfunction, especially in those with Grave's disease or autoimmune inflammation of the thyroid gland.

#### ■ FURTHER READING :

##### BOOKS:

Harrison, J. R., W. Paile, and K. Baverstock. "Public Health Implications of Iodine Prophylaxis in Radiological Emergencies" in: Thomas, G., A. Karaoglou, and E. D. Williams, eds. *Radiation and Thyroid Cancer*. Singapore: World Scientific, 1999.

##### PERIODICALS:

Astakhova, L. N., L. R. Anspaugh, G. W. Beebe, et al. "Chernobyl-Related Thyroid Cancer in Children in Belarus." *Radiation Research* no. 150 (1998): 349–356.

Robbins, J., and A. B. Schneider. "Thyroid Cancer following Exposure to Radioactive Iodine." *Reviews in Endocrine and Metabolic Disorders* no. 1 (2000): 197–203.

##### ELECTRONIC:

U.S. Food and Drug Administration. "Guidance: Potassium Iodide as a Thyroid Blocking Agent in radiation Emergencies." Center for Drug Evaluation and Research. December 10, 2001. <<http://www.fda.gov/cder/guidance/4825fnl.htm>> (April 9, 2003).

U.S. Nuclear Regulatory Commission. "Frequently Asked Questions About Potassium Iodide." National Research

Council. April 2, 2003. <<http://www.nrc.gov/what-we-do/regulatory/emer-resp/emer-prep/ki-faq.html>> (April 12, 2003).

SEE ALSO

*Atmospheric Release Advisory Capability (ARAC)*  
*Chernobyl Nuclear Power Plant Accident, Detection and Monitoring*  
*Nuclear Weapons*

## President of the United States (Executive Command and Control of Intelligence Agencies)

■ JUDSON KNIGHT

As commander in chief, the President of the United States oversees not only all U.S. military forces, but U.S. national security as a whole. In this capacity, the President exercises executive command and control of intelligence agencies, and issues executive orders and presidential directives that shape national security policy. The nation's 14 largest intelligence agencies belong to the Intelligence Community, whose leader, the Director of Central Intelligence (DCI), reports directly to the President. Executive oversight of intelligence also emanates through the National Security Council (NSC) and the President's Foreign Intelligence Advisory Board (PFIAB). The President in turn presents intelligence budgets to the U.S. Congress, which exercises checks and balances on executive power.

### Architect of National Security

The modern age of national security began in 1947, with the passage of the National Security Act, which reorganized the Department of Defense (DOD) and established the Central Intelligence Agency (CIA) and NSC. Prior to that time, the President had always exercised control over the armed forces as commander in chief, but now he also supervised a nascent security and intelligence apparatus destined to grow considerably over the years.

The modern President articulates much of his role as director of national security policy through executive orders and, more recently, presidential directives. Executive orders, which originated under the administration of President Theodore Roosevelt and grew considerably in number after World War II, are theoretically subject to congressional override, but in practice amount to executive edicts. Important executive orders from the 1970s and onward

have addressed issues such as the organization of the Intelligence Community and the handling of classified documents.

Whereas executive orders are open to the public, presidential directives are classified, and knowledge of their content only emerges, if at all, after the fact. These directives have guided security and intelligence policy since the administration of President John F. Kennedy, and each administration has sought to place its own stamp on them by giving them specific titles as a class. For example, they were known as national security directives under George H. W. Bush, presidential decision directives under William J. Clinton, and national security presidential directives under George W. Bush.

In 1986, Congress called on presidents to issue an annual National Security Strategy (NSS), a document outlining the blueprint for national security. Prior to the 2002 NSS of George W. Bush, these usually did little more than simply restate policies then in effect. The Bush NSS, on the other hand, outlined an explicit framework for U.S. actions to be taken in the wake of the September 11, 2001, terrorist attacks.

### The Advisors

In directing intelligence policy, the President relies on Cabinet-level advisors whose departments have a role in national security. Most notable among these are the secretaries of State, Defense, Homeland Security, Energy, and the Treasury, as well as the Attorney General. Other Cabinet officials, including the secretaries of Agriculture, Commerce, and Transportation, also support some national-security functions, and may be called upon for advice relating to their specific areas.

The role of the Vice-President as advisor varies as a function of his relationship with the President. Kennedy, for instance, worked little with Lyndon B. Johnson, whose inclusion on the winning 1960 ticket had resulted from a marriage of convenience designed to attract conservative Southern Democrats. On the other hand, George W. Bush has relied heavily on Vice-President Dick Cheney, who served in the administration of his father.

**The NSC.** The Vice President is, along with the secretaries of State and Defense, a statutory member of the NSC, as is the Chairman of the Joint Chiefs of Staff and the DCI. The chairman of the NSC is the President himself. Intended to serve as the principal advisory board on matters of national security and foreign policy, the NSC has in practice functioned to a level of importance determined by the chief executive.

In general, Democratic presidents have tended to take an *ad hoc* approach to the NSC, while Republicans, starting with Dwight D. Eisenhower, have relied more heavily on the NSC, or at least on the National Security Advisor, who played an important role in the administrations of

Richard M. Nixon, George W. Bush, and others. The role of the National Security Advisor, officially titled the Assistant to the President for National Security Affairs, is not mentioned in the National Security Act, and emerged only during the Kennedy administration.

In addition to the four statutory members, the two statutory advisors on military and intelligence affairs, and the National Security Advisor, the Secretary of the Treasury is a regular attendee at NSC meetings. The Chief of Staff to the President, Counsel to the President, and Assistant to the President for Economic Policy are invited to attend any NSC meeting, while the Attorney General and the Director of the Office of Management and Budget (OMB) are invited to attend those meetings that pertain to their responsibilities. The directors of other executive departments and agencies, as well as other senior officials, are called to attend when appropriate. Under the George W. Bush administration, the Director (later Secretary) of Homeland Security has been a regular participant in NSC meetings.

**PFIAB.** Established by President Eisenhower in 1956, PFIAB is an independent advisory board within the Executive Office of the President. It consists of 16 uncompensated members, selected by the President from outside the ranks of government. PFIAB reviews the activities and performance of all agencies involved in intelligence activities, and advises the President on its assessments of their performance. It also provides the President with input on the objectives, conduct, and coordination of activities by members of the Intelligence Community.

Under the aegis of the PFIAB is the three-member Intelligence Oversight Board (IOB), established by President Gerald Ford in 1976. The IOB is responsible for oversight regarding the legality and propriety of intelligence activities, particularly—according to its charter—those “intelligence activities that the IOB believes may be unlawful or contrary to executive order or presidential directive.” Originally an independent body, the IOB became a standing committee of the PFIAB in 1997.

## The Intelligence Community, Budgeting, and Congress

In addition to leading the CIA, DCI serves as the President’s principal advisor on intelligence matters. He also leads the Intelligence Community, which, along with CIA, includes 13 other agencies within the departments of Defense, State, Energy, Justice, the Treasury, and Homeland Security. Among the members of the Intelligence Community are the Federal Bureau of Investigation, National Security Agency, and Defense Intelligence Agency.

DCI reports to the President both directly and (depending on the operational structure of the administration in question) through the National Security Advisor. As head of the Intelligence Community, DCI presents the

President with the annual Intelligence Community budget, known as the National Foreign Intelligence Program (NFIP).

In preparing the budget for intelligence and national security activities in the coming fiscal year, the President also relies on the Secretary of Defense. The latter presents the President with two budgets: the Joint Military Intelligence Program (JMIP) for military intelligence, and Tactical Intelligence and Related Areas (TIARA) for specific tactical intelligence requirements of the military services.

Using the NFIP, JMIP, and TIARA budgets, the President proceeds to establish an overall DOD intelligence budget with the help of the National Security Advisor and the OMB. He then presents these requests to Congress, which, once it approves the request, passes the annual intelligence authorization act. The latter originated in the late 1970s, as a result of congressional distrust toward the executive branch in the fallout from the Watergate scandal.

Intelligence authorization acts, in addition to numerous mechanisms for direct congressional oversight of intelligence, gives Congress influence over intelligence activities. In the case of the intelligence authorization process, Congress may refuse budgeting for certain requested activities, with the result being a tug-of-war between the White House and Capitol Hill. On the other hand, the President himself may veto intelligence authorization acts, which also include other, non-budgetary, provisions.

### ■ FURTHER READING:

#### BOOKS:

- Andrew, Christopher M. *For the President’s Eyes Only: Secret Intelligence and the American Presidency from Washington to Bush*. New York: HarperCollins, 1995.
- Gore, Albert. *The Intelligence Community: Accompanying Report of the National Performance Review, Office of the Vice President*. Washington, D.C.: U.S. Government Printing Office, 1993.
- Helgerson, John L. *Getting to Know the President: CIA Briefings of Presidential Candidates, 1952–1992*. Washington, D.C.: Central Intelligence Agency, 1996.
- Mann, Thomas E. *A Question of Balance: The President, Congress*. Washington, D.C.: Brookings Institution, 1990.
- Thompson, Kenneth W. *The President, the Bureaucracy, and World Regions in Arms Control*. Lanham, MD: University Press of America, 1998.

#### SEE ALSO

- Executive Orders and Presidential Directives*  
*Intelligence Authorization Acts, United States Congress*  
*Intelligence Community*  
*Intelligence, United States Congressional Oversight*  
*National Security Strategy, United States*  
*NIC (National Intelligence Council)*  
*NSC (National Security Council)*  
*PFIAB (President’s Foreign Intelligence Advisory Board)*  
*Politics: The Briefings of United States Presidential Candidates*  
*United States, Intelligence and Security*

## Pretty Good Privacy (PGP)

■ LEE W. LERNER

PGP, or Pretty Good Privacy, is a security software application used for the encryption and decryption of data. In 1991, Philip R. Zimmermann wrote PGP for the purpose of sending secured data across an insecure network, such as the internet. Individuals, businesses, and governments use strong cryptography programs such as PGP to secure networks, emails, documents, and stored data.

PGP was originally designed as a combination of RSA encryption and a symmetric key cipher known as Bass-O-Matic. RSA is a public key cryptographic algorithm named after its designers Ronald Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm, developed in 1977 (earlier versions of which were partially developed by intelligence agencies), quickly became a major advancement in cryptology. The RSA algorithm depends upon the difficulty in factoring very large composite numbers and is currently the most commonly used encryption and authentication algorithm in the world. The RSA algorithm forms were used in the development of modern Internet web browsers, spreadsheets, email, and word processing programs.

Bass-O-Matic is a conventional (often referred to as symmetric) key algorithm. Bass-O-Matic was later replaced by another conventional key algorithm known as IDEA, which enabled more powerful encryption technology.

Conventional cryptology is based on the concept that one key is used in both the encryption and decryption process. The major benefit of conventional cryptology is the speed in which the encryption process takes place. Conventional encryption can be up to one thousand times faster than public key encryption. However, secure key distribution is a major problem in this form of cryptology.

In 1975, Whitfield Diffie and Martin Hellman developed public key cryptology to increase the security of exchanging keys. Each user of a public key based system has a public and private key. First, the user publishes the public key to a server or contact. Next, the contact encrypts the message to the user's public key. Finally, the user employs the private key to decrypt the cipher text (encoded message) received. The combination of both public and conventional key cryptology makes PGP a hybrid cryptosystem. This allows for users of PGP to be able to securely exchange keys and still have a speedy transaction of secured data.

PGP follows a simple process when encrypting plaintext into cipher text. PGP first compresses the document desired for encryption. This saves modem transmission time and strengthens the cryptographic security of the plaintext. Next, PGP creates a session key. The key is a number correlating to the random movements of the user's mouse and the keys that are typed. The key then works with a cryptographic algorithm to encrypt the plaintext. A cryptographic algorithm is a mathematical

function in which a computable set of steps must be followed to achieve a desired result. The strength of this encryption is dependent on the strength of the algorithm.

After the data has been encrypted into cipher text, PGP encrypts the session key. The session key is encrypted to the recipient's public key. PGP uses digital certificates to prove the identity of a public key. The cipher text and encrypted session key are then transmitted to the recipient. When the recipient receives the data, PGP uses the user's private key to decrypt the session key. When PGP has recovered the session key, it can be used to decrypt the cipher text.

Though the plaintext has been recovered, there is still a question of authentication. PGP uses digital signatures to provide the recipient of an encryption with an origin and identification. Digital signatures are created in the opposite way a public cryptography system works. The sender encrypts a digital signature with their private key and attaches it to the rest of the data transmitted. When the digital signature is received, PGP decrypts it with the sender's public key. Through this process, PGP is able to determine the authenticity of the signature.

Digital signatures produce large amounts of data, slowing transmission and processing speeds. PGP uses a hash function to regulate the amount of data sent. The hash function takes variable amounts of data (the size of the plaintext) and produces a fixed amount called a message digest. PGP then creates a digital signature with the message digest and the user's private key. The hash function also helps to prove the authenticity of the encryption. If the encryption is changed after this process takes place, an entirely new message digest is created. This allows for PGP to detect encryption tampering.

Although PGP encryption has been available to the general public for several years, debate regarding encryption technologies and national security issues, especially in the United States, has ensued. Many government officials argue that strong cryptography programs should not be exported outside the United States. Security algorithms used in PGP type programs were classified as munitions by the United States government. As such, they remained subject to severe export control and restrictions that inhibited their widespread distribution and use. Due to these concerns, there are presently two available PGP applications: PGP and PGPi (international). Any user outside of the United States is currently required to utilize PGPi.

The National Institute of Standards and Technology (NIST), oversees the development of many cryptography standards. One such standard, developed by commercial entities and the United States National Security Agency (NSA) in the 1970s was termed the Data Encryption Standard (DES). In anticipation of increasing security needs, in the late 1990s, NIST began to work toward the implementation of the Advanced Encryption Standard AES to replace DES.



## ■ FURTHER READING :

### BOOKS:

Kaufman, Charles, et. el. *Network Security: Private Communication in a Public World*, 2nd. ed. Upper Saddle River, NJ: Prentice Hall, 2002.

Stallings, William. *Cryptography and Network Security: Principles and Practice*, 3rd. ed. Upper Saddle River, NJ: Prentice Hall, 2002.

Zimmerman, Phillip. *The Official PGP User's Guide* Cambridge, MA: MIT Press, 1995.

### SEE ALSO

*Computer and Electronic Data, Destruction*

*Computer Fraud and Abuse Act of 1986*

*Computer Hackers*

*Computer Hardware Security*

*Computer Security Act (1987)*

*Computer Software Security*

*Computer Virus*

*Cryptology and Number Theory*

*Cyber Security*

*Encryption of Data*

## Privacy: Legal and Ethical Issues

### ■ JUDSON KNIGHT

Among the foundational principles of the Western liberal tradition that binds the American political system is the belief that the rights of the individual, wherever possible, must be preserved against the authority of the state. Emanating from that principle is the implication that individuals have a right to privacy, a right implied—as noted by several distinguished Supreme Court justices over time—in the U.S. Constitution. Balancing and sometimes apparently contradicting this right to privacy is the need for security on a national and sometimes a local level. This conflict of needs and aims has given rise to public debate over numerous specific issues, including national security measures undertaken in the wake of the September 11, 2001, terrorist attacks.

### Privacy Rights in Tort and Constitutional Law

A wide array of U.S. laws, both tort and constitutional, support the individual's right to privacy. In tort law, persons have a right to seek legal redress for invasions of privacy undertaken for the purposes of material gain, mere curiosity, or intention to defame. These protections

extend to all persons under U.S. law, though public figures—a term strictly defined in legal statutes—have somewhat less broad rights of privacy.

Some national constitutions spell out the rights of the individual, with the assumption that all other privileges belong to the government. The U.S. Constitution, by contrast, delineates government authority, with the provision that all other rights belong to individuals. To James Madison and other founders of the republic, these guarantees did not go far enough, and therefore, Congress passed the Bill of Rights, or the first 10 amendments to the Constitution. Among these are several that would later figure heavily in debates over privacy: the First Amendment, with its protection of free speech; the Fourth Amendment, against unlawful search and seizure; and the Fifth Amendment, which provides for due process under law. The Fourteenth Amendment, passed after the Civil War to protect the rights of freed slaves, extends Fifth Amendment provisions to states as well.

Contrary to popular belief, neither the Constitution nor its amendments contain any reference to privacy as a right *per se*. The concept of “The Right to Privacy” comes from an influential 1890 *Harvard Law Review* article by that title, under which Supreme Court Justice Louis Brandeis, writing with Samuel Warren, put forward the proposition that privacy rights extend beyond mere protection against clear-cut intrusions on privacy. Thereafter, a number of landmark decisions in the Supreme Court broadened the concept of privacy as defined in constitutional law. Among these was *Griswold v. Connecticut* (1965), involving a state law that prohibited the use of contraceptives. Writing for the Court, which struck down the law, Justice William O. Douglas held that the “penumbra” of the First, Fourth, and Fifth collectively provides a “zone of privacy”.

### The Revolution of the 1970s

The 1970s saw a revolution in privacy rights, not only through the Court—whose *Griswold* decision set the stage for the protection of abortion rights in *Roe v. Wade* (1973)—but also in the legislative branch of government. In 1974, Congress passed the Privacy Act, which restricts the authority of government agencies to collect information on individuals or to disclose that information to persons other than the individual. The Privacy Act also requires agencies to furnish the individual with any information on him or her that the agency had in its files.

In 1967, Congress had passed the Freedom of Information Act (FOIA), which limits the ability of U.S. federal government agencies to withhold information from the public by classifying that information as secret, but it greatly expanded FOIA provisions in 1975. Together with the Privacy Act—the two are often referred to collectively as the Freedom of Information-Privacy Acts (FOIPA)—these served to further extend the rights of individuals

against government intrusion. Like FOIA, the Federal Wiretapping Act of 1968 had been passed earlier, but it, too, was extended in the 1970s. (Today, all U.S. states have laws against wiretapping and telephone recording.)

Many of these changes occurred as a response, either directly or indirectly, to the Watergate scandal and the subsequent revelations of illegal wiretapping, recording, and surveillance activity conducted by the Nixon White House and other compartments of the federal government. In 1976, Congress passed the Foreign Intelligence Surveillance Act (FISA). FISA, which became law in 1978, placed checks and balances on the authority of government agencies to conduct surveillance on persons accused of conducting espionage—authority that had been misused by Federal Bureau of Investigation director J. Edgar Hoover in some domestic intelligence campaigns during the 1950s and 1960s.

## Privacy Issues in the 1990s and Beyond

In September, 1997, Congress passed the Fair Credit Reporting Act (FCRA), which requires potential employers to obtain written authorization from a job candidate or employee before accessing records from a consumer reporting agency. The employer is also required to notify the employee or applicant if any adverse action is taken pursuant to a negative report. Thus federal law extended privacy rights to protect the individual from intrusion by businesses as well as the government.

Many privacy issues at the dawn of the twenty-first century involved new technologies and new developments in the national security environment. In the area of technology, the broadening of access to the Internet brought with it a number of concerns regarding government monitoring of e-mail and other traffic—concerns heightened by the revelation, in the late 1990s, that the National Security Agency and counterparts in other parts of the English-speaking world monitor global communications through the Echelon surveillance system. On the one hand, the Internet has provided new venues for illegal activity such as the dissemination of child pornography; on the other hand, groups such as the American Civil Liberties Union (ACLU) contend that government monitoring of such activities is often used against innocent persons.

The ACLU has been among the most vocal opponents to intensified security measures undertaken in the wake of the September 2001 bombings. In October 2001, Attorney General John Ashcroft presented a proposed antiterrorism bill that would broaden government authority under FISA. Questioning these and other measures, ACLU spokespersons, acknowledging the need for heightened security, stated that the ACLU's goal is to monitor the proposal for increased law enforcement power to ensure that they have maximum effectiveness with a minimal erosion of civil liberties."

## ■ FURTHER READING:

### BOOKS:

- Alderman, Ellen, and Caroline Kennedy. *The Right to Privacy*. New York: Knopf, 1995.
- Branscomb, Anne W. *Who Owns Information? From Privacy to Public Access*. New York: Basic Books, 1994.
- Diffie, Whitfield, and Susan Eva Landau. *Privacy on the Line: The Politics of Wiretapping and Encryption*. Cambridge, MA: MIT Press, 1998.
- Harrison, Maureen, and Steve Gilbert. *Landmark Decisions of the United States Supreme Court*. Beverly Hills, CA: Excellent Books, 1991.
- Henderson, Harry. *Privacy in the Information Age*. New York: Facts on File, 1999.
- Rosen, Jeffrey. *The Unwanted Gaze: The Destruction of Privacy in America*. New York: Random House, 2000.

### SEE ALSO

*Cameras*  
*Computer Keystroke Recorder*  
*Domestic Intelligence*  
*Echelon*  
*FOIA (Freedom of Information Act)*  
*Foreign Intelligence Surveillance Act*  
*Genetic Information: Ethics, Privacy and Security Issues*  
*Internet Surveillance*  
*Pretty Good Privacy (PGP)*  
*Security Clearance Investigations*  
*Telephone Caller Identification (Caller ID)*  
*Telephone Recording Laws*  
*Telephone Recording System*  
*Telephone Scrambler*  
*Telephone Tap Detector*  
*Watergate*

---

## Profiling

---

### ■ JUDSON KNIGHT

Profiling is the process of developing descriptions of the traits and characteristics of unknown offenders in specific criminal cases. It is often used in situations for which authorities have no likely suspect. There are two basic varieties of profiling: inductive, which involves the development of a profile based on known psychological typology; and deductive profiling, which reasons exclusively from the details of the victim and crime scene to develop a unique profile. Profiling as a law enforcement tool emerged in the late 1960s, and today, the leading entity engaged in profiling is the National Center for the Analysis of Violent Crime (NCAVC) of the Federal Bureau of Investigation (FBI).

Profiling should not be confused with *racial profiling*. Racial profiling, a topic surrounded with considerable controversy, came to the forefront in the late 1980s and

1990s, when a number of activists and social scientists maintained that law enforcement officials tended to single out African Americans, particularly young males, for arrest and abuse. After the September, 2001, terrorist attacks, random searches and other forms of attention directed toward against Middle Eastern males were also decried in some quarters as racial profiling.

In contrast to the socially explosive topic of racial profiling, criminal profiling—while it may be controversial among law enforcement authorities and forensic scientists, not all of whom agree on its merits or the proper approach to it—is not controversial in society at large. In fact, television programs concerning crime, as well as dramatic portrayals in popular films have raised considerable public interest in profiling. Thanks to this interest, leading profilers are well-known outside the law-enforcement community.

**Misconceptions.** Indicative of this popularity was the prominence given to profiling opportunities on a frequently asked questions (FAQ) page in the employment section of the FBI's Web site in 2003. Alone among FBI specialties, profiling was featured with the question "I just want to be an FBI 'profiler.' Where do I begin the application process?" As the bureau noted in its response, "You first need to realize the FBI does not have a job called 'Profiler.'" The answer went on to discuss the NCAVC, located at FBI headquarters in Quantico, Virginia. The FBI also noted on the site that "these FBI Special Agents [involved in profiling] don't get vibes or experience psychic flashes while walking around fresh crime scenes. [Instead, profiling] is an exciting world of investigation and research. . . ."

**Two varieties of profiling.** Criminal profiling originated from the work of FBI special agents Howard Teten and Pat Mullany in the late 1960s. It is especially used in cases involving serial killers, who usually are not personally acquainted with their victims. Most murders involve people who know one another, and in most murder investigations, likely suspects can be readily identified. For example, if a married woman is murdered, her husband often quickly becomes the focus of police investigation. If, however, there is nothing to suggest that a victim has been murdered by someone he or she knows, or if the victim's identity is unknown, profiling may be necessary in order to develop a set of leads for investigators.

Criminal profilers make use of two types of reasoning, which, in the view of some profiling experts, constitute two schools of thought. Inductive criminal profiling, like the larger concept of induction in the philosophical discipline of epistemology (which is concerned with the nature of knowledge) develops its portrait of a suspect based on the results gathered from other crime scenes. Inductive criminal profiles draw on formal and informal

studies of known criminals, on the experience of the profiler, and on publicly available data sources, to provide guidance.

By contrast, deductive criminal profiling relies purely on information relating to the crime scene, the victim, and the evidence. Instead of drawing on the facts of other crimes, the deductive profile draws only on the information relating to the crime in question. For instance, if a search of the crime scene reveals that the killer had smoked an expensive variety of cigar, this would lead the deductive profiler to posit that the killer was wealthy and probably well educated. The profiler working through pure deduction would not, however, seek to compare this fact with information on other killers in the past who had smoked expensive cigars.

**NCAVC and VICAP.** FBI profilers are supervisory special agents with NCAVC. In order to be considered for the program, an individual must have served as an FBI special agent for three years. However, due to high competition for placement in the program, individuals selected usually have eight to 10 years of experience with the bureau. Newly assigned personnel typically undergo a structured training program of more than 500 hours. Alongside these special agents work other, civilian, personnel in positions that include intelligence research specialist, violent crime resource specialist, and crime analyst. It is their job to research violent crime from a law enforcement perspective, and to provide support to NCAVC special agents.

In addition to developing criminal profiles, NCAVC provides major case management advice and threat assessment services to law-enforcement officials around the nation and the world. Special agents may also provide law enforcement officials with strategies for investigation, interviewing, and prosecution. Among the services provided by NCAVC to the law enforcement community at large is VICAP, the Violent Criminal Apprehension Program.

VICAP is a nationwide data information center tasked with collecting, collating, and analyzing information on violent crimes, particularly murder. Cases eligible for VICAP include solved or unsolved homicides or attempts, especially ones involving an abduction; apparently random, motiveless, or sexually oriented homicides; murders that are known or suspected to be part of a series (i.e., serial murder); unresolved missing persons cases, particularly those in which foul play is suspected; and unidentified dead bodies for whom the manner of death is known or suspected to be homicide.

Local law enforcement agencies participating in VICAP are able to draw on its information database in solving crimes. For example, if a murder were committed with a rare variety of handmade pistol, VICAP could be consulted for information on other cases involving such a weapon. Once a case has been entered into the VICAP database, it is compared continually against all other entries on the basis

of certain aspects of the crime. VICAP has been used to solve a number of homicides nationwide.

#### ■ FURTHER READING:

##### BOOKS:

Ainsworth, Peter B. *Offender Profiling and Crime Analysis*. Portland, OR: Willan, 2001.

Evans, Collin. *The Casebook of Forensic Detection: How Science Solved 100 of the World's Most Baffling Crimes*. New York: Wiley, 1996.

Holmes, Ronald M. *Profiling Violent Crimes: An Investigative Tool*. Newbury Park, England: Sage Publications, 1989.

Turvey, Brent E. *Criminal Profiling: An Introduction to Behavioral Evidence Analysis*. San Diego, CA: Academic Press, 1999.

##### ELECTRONIC:

Federal Bureau of Investigation. <<http://www.fbi.gov>> (May 4, 2003).

##### SEE ALSO

*FBI (United States Federal Bureau of Investigation) Forensic Science Intelligence and Counter-Espionage Careers Justice Department, United States*

---

## Propaganda, Uses and Psychology

---

#### ■ CARYN E. NEUMANN

Propaganda is a form of communication that attempts to influence the behavior of people by affecting their perceptions, attitudes and opinions. Propaganda can restructure hostile attitudes, reinforce friendly attitudes, or maintain the continued neutrality of those people who are undecided. A characteristic of propaganda is its reliance upon devices designed to discourage reflective thought such as name calling, use of glittering generalities like “freedom” or “injustice,” use of prestigious symbols, endorsements from prominent persons, endorsements from regular folk, get-on-the-bandwagon representations, and cardstacking to minimize or maximize events. Propaganda does not always advance an argument and is often aimed instead at advancing an image or general system of ideas that implicitly supports an action or policy.

While propaganda has existed for ages, the advent of twentieth century mass communication enabled it to flourish and it has been employed with increasing sophistication in all major conflicts beginning with World War I.

Unlike other forms of warfare, the success or failure of propaganda cannot be immediately known or measured. It is a continuous process that persuades without seeming to do so. The sources and accuracy of propaganda mark it as being one of three forms: white, black, or gray.

White propaganda comes from a source that is identified correctly and the information in the message tends to be accurate. The Voice of America (VOA) is an example of a white propaganda unit because it presents a positive image of the United States. While the VOA is not connected with the military, armed forces have commonly used radio to destroy the enemy’s will to resist with a minimum loss of blood. During the 1991 Persian Gulf War, the U.S. Fourth Psychological Operations Group produced a white propaganda radio program that featured testimonials from happy Iraqi prisoners of war along with prayers from the Koran and the location of U.S. bomb targets for the next day. A great majority of Iraqi defectors said that the broadcasts influenced their decision to surrender. White propaganda attempts to build credibility with the audience by convincing them of the good intentions of the sender.

Black propaganda, from a source that is often well concealed, employs a high number of distortions or outright falsehoods. It is also categorized as disinformation, from the name of a KGB division, *dezinformatsia*, that specialized in such a form of creative deceit. In World War I, Germany made a crude and futile attempt to persuade French soldiers at the front to abandon their units by posting large signs advising them that British men were engaging in sexual relations with the soldiers’ wives. By World War II, the same sort of message designed to demoralize troops received more polish through the transmissions of Lord Haw Haw and Tokyo Rose. A similar style of disinformation came in the form of “The New England Broadcasting Station.” This station, supposedly run by discontented British subjects, began sending radio transmissions of war news in the weeks prior to the planned invasion of England by Germany. The station was actually an undercover German operation that aimed to reduce the morale of the British people. Black propaganda seeks to destroy the credibility of opposition governments.

Gray propaganda may or may not be correctly identified and the accuracy of the information is uncertain. In the aftermath of the failed 1961 CIA-led Bay of Pigs invasion, the VOA denied any American involvement. While the source of the information was clearly identified as the VOA, the information was false. Sometimes gray propaganda is true and designed to embarrass an enemy. During the Cold War, the Soviet Union used examples of American racism, such as lynchings, to slow U.S. advances throughout Africa, Asia, and Latin America. The damage that this gray propaganda caused to foreign relations ultimately prompted the U.S. government to back domestic civil rights legislation.

By turning enemies into friends or neutrals through the power of persuasion, propaganda offers a relatively



A crowd of people read the displayed information at the Nazi propaganda exhibition in Munich, Germany, in 1937. ©HULTON-DEUTSCH COLLECTION/CORBIS.

inexpensive way of reducing armed conflict and bolstering national security. For this reason, it will most likely remain a popular weapon in government arsenals.

#### ■ FURTHER READING :

##### BOOKS:

Dudziak, Mary L. *Cold War Civil Rights: Race and the Image of American Democracy*. Princeton: Princeton University Press, 2000.

Jowett, Garth S., and Victoria O'Donnell. *Propaganda and Persuasion*. Thousand Oaks, CA: Sage Publications, 1999.

Sproule, J. Michael. *Channels of Propaganda*. Bloomington, IN: EDINFO Press, 1994.

##### SEE ALSO

*Bay of Pigs*  
*Black Ops*  
*CIA (United States Central Intelligence Agency)*  
*Cold War (1945–1950): The start of the atomic age*  
*Cold War (1950–1972)*

##### *Disinformation*

##### *Information Warfare*

*KGB (Komitet Gosudarstvennoi Bezopasnosti, USSR Committee of State Security)*

##### *Lord Haw-Haw*

##### *Persian Gulf War*

##### *Tokyo Rose*

*Voice of America (VOA), United States*

## Pseudoscience Intelligence Studies

#### ■ JUDSON KNIGHT

During the 1960s, Soviet intelligence services became interested in the possible use of paranormal abilities for “psychic intelligence” or “remote viewing”—the use of

telekinetic powers to glimpse or otherwise comprehend objects not immediately available to the senses. Remote viewing, it was claimed, would help intelligence officers gain access to information that could not be seen or heard by ordinary means. U.S. intelligence officials, particularly in the Defense Intelligence Agency (DIA), learned of the Soviet interest, and themselves became fascinated with remote viewing. The result was a \$20 million DIA program known as Stargate, which lasted throughout the 1980s. Ultimately red-flagged by CIA, Stargate in its heyday attracted considerable respect within sectors of the U.S. intelligence community.

## Soviet Experiments in the 1960s

The catalyst for American interest in pseudoscientific intelligence methods was the publication, in 1970, of *Psychic Discoveries Behind the Iron Curtain*. According to authors Sheila Ostrander and Lynn Schroeder, a number of Soviet scientists were interested in various aspects of the paranormal, including telekinesis, extrasensory perception (ESP), parapsychology, and various other psychic phenomena. These scientists had worked with military and intelligence agencies in their country to explore methods for deployment of paranormal abilities for defense and intelligence-collection purposes.

Among the most intriguing stories included in the book was an account of an experiment involving rabbits. Electrodes were inserted into the brain of a mother rabbit, and baby rabbits—without implanted electrodes—were placed on a submarine that was then taken out to sea and submerged. A baby rabbit was killed, and as the scientists recorded, the brain of the mother, many miles away on shore, reacted at the moment of death. Setting aside all questions of animal cruelty and experimental ethics, the was interpreted to show that ESP existed and served to connect minds.

## Early CIA Experiments

*Psychic Discoveries* elicited considerable interest in the use of the paranormal for intelligence-gathering, but U.S. programs in psychic intelligence seem to have started much earlier, probably sparked by an awareness of Soviet activities in this area. The CIA conducted its own experiments with remote viewing through its Directorate of Science and Technology (DS&T), beginning in the mid-1960s, and continuing for many years thereafter.

During the early part of this period, Carl Duckett, who became CIA Deputy Director for Science and Technology in 1966, funded remote viewing experiments at the Stanford Research Institute (SRI) in California. Remote viewers at SRI attempted to locate targets of interest in the Soviet Union, and in other nations whose nuclear capabilities were a matter of concern to the United States.

**Evaluating results.** In late 1975, a team at Los Alamos National Laboratory conducted a study of one experiment, in which remote viewer Pat Price evaluated a site under investigation by both the CIA (which called it URDF-3, or Unidentified Research and Development Facility-3) and the Air Force, which referred to it as PNUTS, or Possible Nuclear Underground Test Site. The Los Alamos evaluator compared Price's "findings" with those obtained by satellite photography.

On the positive side, Price had "seen" a gantry crane that was actually there, but he had also discerned nine other objects whose presence the satellite revealed to be fictional. According to the Los Alamos report, from December 1975, "the validity of Price's remote viewing of URDF-3 appears to be a failure." Years later, after the end of the Cold War, American scientists had an opportunity to view the site firsthand, and learned that it was concerned with developing nuclear-powered rockets for space flight.

**DIA and Stargate.** During the late 1970s, DIA began developing a project codenamed Grillflame, which ultimately became Stargate. The connection between *Psychic Discoveries* and Stargate is not a clear one, but Pentagon officials did examine the book, and Stargate seems to have been a U.S. response to Soviet efforts.

At the time of the book's publication, DIA was a young agency attempting to prove itself within the Intelligence Community. Formed in 1961, it had not fared well during the Vietnam War, when it faced considerable intransigence from the intelligence agencies of the various military services. The idea of using unorthodox means to gain intelligence was seen by some personnel to offer a way of gaining a competitive edge within the Intelligence Community.

Although lacking in scientific evidence, Stargate drew in a number of respectable intelligence organizations—not just DIA, but also the National Security Agency (NSA), which in September, 1979, requested remote viewers' help with regard to Soviet submarine construction projects. One remote viewer produced a surprisingly accurate reading, predicting the launch of a new sub in 100 days. In fact the craft was glimpsed 120 days later, but it had fewer than the 18 to 20 missile launch tubes predicted by the remote viewer. Skeptics of remote viewing point out that "hits" were often based upon clues given to "viewers" and that misses were numerous.

In fairness to Stargate, it should be noted that Joseph McMoneagle, one of the chief remote viewers, later said that all readings by remote viewers were intended merely to augment, not supplant, intelligence gained by more conventional means. Additionally, the NSA, the Joint Chiefs of Staff, the Drug Enforcement Administration, Secret Service, Customs Bureau, and Coast Guard requested readings from Stargate remote viewers. So, too, did the CIA, but in the mid-1990s the agency took over the program, had it evaluated scientifically, then cut off funding.

In 1995, as a result of an executive order by President William J. Clinton authorizing the declassification of certain materials, information on both the SRI program, initiated in 1972, and Stargate became public. Both programs appear to have lasted into the early 1990s, and when this information became public, many observers wondered just how the Intelligence Community could have invested so much money in such fanciful activities.

One explanation was the cultural environment of the United States at the time—an influence to which intelligence officials are not necessarily any less susceptible than ordinary citizens. The 1970s was the heyday of the paranormal, the occult—Satanism made the cover of *Time* magazine in 1972—and what scientists would describe as pseudoscience. Israeli psychic Uri Geller appeared to bend spoons with his mind on television, and popular TV programs such as *In Search of . . .* (hosted by *Star Trek's* Leonard Nimoy) treated outlandish notions with the utmost of seriousness.

Despite the best efforts of professional skeptics like James Randi to expose the fraud in pseudoscience, the fascination with bizarre programs continued. During the 1970s, bestsellers such as Erik von Daniken's *Chariots of the Gods* promised evidence that extraterrestrial visitors had left countless clues of their ancient journeys to Earth at sites such as the Great Pyramids in Egypt. Interest in Nostradamus's writings swelled, and religious cults flourished. It was an ideal time for experimentation in psychic intelligence-gathering, and thus, it seems to be no accident that the CIA and DIA programs took place during this period.

Additionally, there was the desire, noted earlier, to keep up with the Soviets. Herein lies an irony. Though the United States would attempt to develop its own psychic intelligence programs in competition with the Soviet Union, it appears that the Soviets were only trying to keep up with the Americans in the first place. *Psychic Discoveries* noted that Soviet experiments were sparked by a 1959 report in the French magazine *Constellation* regarding alleged telepathy experiments conducted by the U.S. Navy. The article, "Thought Transmission—Weapon of War," was based on a misreading or misunderstanding of Navy activities. Therefore it is possible to characterize experiments in psychic intelligence on both sides of the iron curtain as, to some degree, a comedy of errors.

#### ■ FURTHER READING:

##### BOOKS:

Mandelbaum, W. Adam. *The Psychic Battlefield: A History of the Military-Occult Complex*. New York: St. Martin's Press, 2000.

Morehouse, David. *Psychic Warrior: Inside the CIA's Stargate Program: The True Story of a Soldier's Espionage and Awakening*. New York: St. Martin's Press, 1996.

Ostrander, Sheila, and Lynn Schroeder. *Psychic Discoveries Behind the Iron Curtain*. Englewood Cliffs, NJ: Prentice-Hall, 1970.

##### ELECTRONIC:

Haines, Gerald K. A Die-Hard Issue: CIA's Role in the Study of UFOs, 1947–90. *Studies in Intelligence* 1, No. 1, 1997. Central Intelligence Agency. <<http://www.cia.gov/csi/studies/97unclass/ufo.html>> (April 28, 2003).

Richelson, Jeffrey T. Science, Technology and the CIA. National Security Archive, George Washington University. <<http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB54/index2.html>> (April 24, 2003).

UFOs. Central Intelligence Agency FOIA. <<http://www.foia.cia.gov/ufo.asp>> (April 28, 2003).

##### SEE ALSO

*Area 51 (Groom Lake, Nevada)*

*CIA (United States Central Intelligence Agency)*

*CIA Directorate of Science and Technology (DS&T)*

*DIA (Defense Intelligence Agency)*

## Pseudorandom Number Generators (PNGs).

SEE *Cipher Pad*.

---

## Psychotropic Drugs

---

■ JUDYTH SASSOON

Psychotropic drugs are a loosely defined grouping of agents that have effects on psychological function and include the antidepressants, hallucinogens, and tranquilizers. They are all compounds that affect the functioning of the mind through pharmacological action on the central nervous system. Psychotropic drugs are ubiquitous in our society and encompass both prescription psychiatric medications and illegal narcotics, as well as many over the counter remedies. Because these compounds affect human behavior, there is much suspicion, misunderstanding, and controversy surrounding their use. Sedative drugs first appeared in the late 1800s. They were followed by barbiturates and amphetamines in the early 1900s. But it was drugs such as chlorpromazine hydrochloride (Thorazine) and lithium, introduced in the 1950s that dramatically affected psychiatric medicine. Medicine essentially recognizes four main psychotropic drug categories: antipsychotics, mood stabilizers, antianxiety agents and antidepressants.

Antipsychotics include chlorpromazine, which was released in 1954 for the treatment of schizophrenia. Originally designated as a major tranquilizer, it was also found

to be effective in subduing the hallucinations and delusions of psychotic patients. Since then, other antipsychotics, including haloperidol (Haldol) and clozapine (Clozaril) were developed for the treatment of various kinds of psychosis. Mood stabilizers were first recognized following Australian psychiatrist John F. J. Cade's 1949 discovery of the beneficial effects of lithium on manic-depressive disorder. Patients with schizophrenia, however, did not respond to lithium, leading psychiatrists to a degree of diagnostic precision that was previously not possible. Recently, some antiepileptic medicines—valproic acid (Depakene) and carbamazepine (Epilex, Tegretol) have also been used to treat manic-depressive disorder. Barbiturates were widely prescribed before the 1960s to relieve anxiety, but were found to be highly sedating and addictive and did not always work successfully. Chlordiazepoxide (e.g. Librium) and the other benzodiazepine agents developed from the 1960s to the 1980s rapidly replaced barbiturates. Antidepressants are possibly the most widely used psychotropic drugs in the United States. In any given 6-month period, about 3 percent of adult Americans experience severe depression. For the millions whose depressed mood becomes a clinical syndrome, though, psychotropic therapy is one way to relieve the symptoms. The tricyclic imipramine hydrochloride (Tofranil), developed during the late 1950s and introduced during the early 1960s, was the first of the now-available antidepressants and still is often prescribed. Research has progressed considerably since then and current theories attribute depression to psychological causes (e.g. low self-esteem, important losses in early life, history of abuse) and biological causes (e.g. imbalance of neurotransmitters, including serotonin and dopamine; disruptions in the sleep-wake cycle) as well as experiential and social factors. The various classes of antidepressants, tricyclics, MAOIs, serotonin-specific agents, and individual drugs including nefazodone (Serzone), mirtazapine (Remeron), venlafaxine (Effexor), and bupropion hydrochloride (BuSpar) target the biological causes. At present, the selective serotonin reuptake inhibitors (SSRIs) hold center stage, and fluoxetine hydrochloride (Prozac) is in the spotlight. The result of years of focused research and design, fluoxetine was rapidly accepted and prescribed to millions within a few months after its introduction in December 1987.

**Psychotropic drugs and law enforcement.** Though much of the research and understanding of psychopharmacology comes from the field of medicine and psychiatry, there are of course, other areas where psychotropic drugs have been used, ranging from illegal recreational use to the possibility of applying them as agents of "mind control." The Central Intelligence Agency (CIA) Crime and Narcotics Center monitors, reviews, and delivers information about international trafficking in illegal drugs and international organized crime to the nation's leaders and law enforcement agencies. Former Director of Central Intelligence William Webster created what became today's DCI Crime

and Narcotics Center in April 1989. The center is staffed by people from the 13 agencies making up the US Intelligence Community, including the CIA, as well as from law enforcement agencies. The Crime and Narcotics Center's staff are responsible for estimating the amount of illegal drugs, mainly coca, opium poppy, and marijuana, produced around the world. They also assist law enforcement agencies to break up drug and organized crime groups and help law enforcement agencies detect and capture illegal drug shipments.

The CIA's interest in psychotropic drugs does not end in law enforcement, however. MK-ULTRA was a CIA "mind-control" project backed during the Cold War years. Because the Soviets were supposedly researching a drug that could be used as a "truth serum," the CIA set out to beat them with heavily-funded research into consciousness altering drugs, and techniques of behavioral control. More recently, following the September 11, 2001, attacks on the World Trade Center in New York by al-Qaeda, there has been some discussion among some CIA and FBI staff, including William Webster, about the use of "truth drugs" to extract information from uncooperative terrorist suspects. United States Secretary of Defense Donald Rumsfeld asserted that narcoanalysis is not used by United States military and intelligence personnel, but suggested that other countries have made use of the technique in the interrogation of suspected terrorists. One such drug is sodium pentothal, which is used as a sedative and anaesthetic during surgery. It depresses the central nervous system, slows the heart rate and lowers blood pressure. Patients on whom the drug is used as an anaesthetic are usually unconscious less than a minute after it enters the veins. Because of its effectiveness as a sedative, it was also one of the first of three drugs to be used by the U.S. prison system during executions. In milder doses, the drug affects people such that they often become more communicative and share their thoughts without hesitation. Despite its name, however, sodium pentothal will not make a person tell the truth against their will; a recipient is only likely to lose inhibitions and therefore, may be more likely to volunteer the truth.

According to conventions set forth by the United Nations, the FBI and other U.S. law enforcement agencies disavow the practice of physically coercing or drugging prisoners, but point to the fact that many other countries around the world utilize drugs in interrogations. U.S. officials prefer to use psychology and investigative knowledge to extract information. Authorities are officially focused on making sure they obtain information without violating a suspect's constitutional rights because they do not want to jeopardize having such evidence ruled inadmissible in court. In attempting to prevent future acts of terrorism, however, authorities are sometimes focused more on obtaining quality information than they are on preparing cases for court, thus, in the present political situation, the FBI may be considering more aggressive methods of interrogation of terrorist suspects that might involve the use of psychoactive drugs.



A recent alleged use of a psychotropic drug by the U.S. was reported in the Russian newspaper, *Komsomolskaya Pravda*. In April 2001, it was reported that U.S. spies used drugged cookies and drinks to break the will of a Russian defense employee and recruit him as an agent. The employee was identified as a 58-year-old worker of a defense ministry facility near Zhukovsky air base, the Russian air force's top flight test center near Moscow. Whether accurate or not, the article illuminates the fact that the U.S. and Russia continue to show interest in spying on each other, despite better relations, and that psychotropic drugs may still play a part in espionage.

#### ■ FURTHER READING :

##### BOOKS:

Maxmen, Jerrold S., and Nicholas G. Ward. *Psychotropic Drugs: Fast Facts*, 2nd ed. N.p., Norton & Company, 1995.

##### PERIODICALS:

Romanko, J. R. "Truth Extraction." *New York Times Magazine*. (November 19, 2000): 54.

##### SEE ALSO

*Chemistry: Applications in Espionage, Intelligence, and Security Issues*  
*CIA (United States Central Intelligence Agency)*  
*FBI (United States Federal Bureau of Investigation)*

## Public Health Service (PHS), United States

#### ■ BELINDA ROWLAND

The United States Public Health Service is a federal government agency that promotes the health of the people of the United States and the world. It is a principle component of the Department of Health and Human Services (HHS) and is composed of eight agencies. Among other duties, the Public Health Service is charged with, through its agencies, preparing for and leading the nation's medical response to a threat or disaster, whether naturally occurring or an act of terrorism.

The PHS originated in 1798 through the passage of an act that provided for the care of injured and sick merchant seamen. Politicians of the time assumed that healthy seamen would protect the security and economic well being of the country. A marine hospital fund was created to provide medical services to merchant marines. Monies

for this fund came, in part, from an American seaman tax of 20 cents each month. This became the first program for medical insurance in the United States. Marine hospitals were established along coasts and inland waterways. By 1981, all of the marine hospitals and clinics had closed.

In 1870, the independently controlled network of hospitals was organized into the Marine Hospital Service. The Service was administered by the Supervising Surgeon General, a title that was later changed to Surgeon General. At this time, the Service developed a military organization and approach. The medical officers were called surgeons and had to pass entrance exams and wear uniforms. In 1889, legislation to formalize the uniformed service aspect of the Service created the Commissioned Corps. As a result, medical officers were given military titles and pay.

By the late 1800s, the activities of the Marine Hospital Service extended beyond the care of seamen. In the effort to control infectious disease, the Service was given the power to quarantine and was responsible for the medical examinations of immigrants. As a result of its expanding responsibilities, in 1902 the name of the service was changed to the Public Health and Marine Hospital Service. The name "Public Health Service" was adopted in 1912.

The PHS celebrated its 200th anniversary in 1998. At that time, it employed about 5,700 Commissioned Corps officers and 51,000 civilians. In 1993, the budget of the PHS was 17 billion dollars. The PHS is administered by the Assistant Secretary for Health and the Surgeon General. It is composed of the Office of Public Health and Science, 10 Regional Health Administrators, and eight agencies. The eight agencies within the PHS are:

- Centers for Disease Control and Prevention (CDC). The mission of the CDC is to promote health through the prevention and control of disease, injury, and disability. The CDC functions on both national and international levels.
- Agency for Toxic Substances and Disease Registry (ATSDR). The ATSDR mission is to prevent the exposure to and adverse effects of toxic substances in the environment.
- National Institutes of Health (NIH). The NIH is a medical research center that conducts and funds medical research with the goal of achieving better health for the people of the United States and the world. It is composed of 27 Institutes and Centers and is one of the world's leading medical research centers.
- Food and Drug Administration (FDA). The FDA assures the safety and effectiveness of drugs, medical devices, and biological products as well as the safety of cosmetics and foods.
- Substance Abuse and Mental Health Services Administration (SAMHSA). SAMHSA strives to reduce the illness, disability, death, and costs resulting from mental illness and substance abuse.
- Health Resources and Services Administration (HRSA). The HRSA directs national health programs which assure that the American people have equal access to healthcare.

- Agency for Healthcare Research and Quality (AHRQ). The AHRQ funds research intended to improve the quality and outcome of healthcare, examine medical errors, address patient safety, and expand access to effective healthcare. It provides information to persons so that they can make better healthcare decisions.
- Indian Health Services (IHS). The IHS is the healthcare provider and advocate for Alaska Natives and American Indians.

## ■ FURTHER READING :

### BOOKS:

- Kondratas, R. *Images from the History of the Public Health Service*. N.p., U.S. Department of Health and Human Services, Public Health Service, 1994.
- Kurian, G. T., ed. *A Historical Guide to the U.S. Government*. New York: Oxford University Press, 1998.
- Mullan, F. *Plagues and Politics: The Story of the United States Public Health Service*. New York: Basic Book, Inc., 1989.

### ELECTRONIC:

- Kondratas, R. "Images from the History of the Public Health Service." April 27, 1998. <[http://www.nlm.nih.gov/exhibition/phs\\_history/contents.htm](http://www.nlm.nih.gov/exhibition/phs_history/contents.htm)> (December 14, 2002).
- Office of the Public Health Service Historian, 18–23 Parklawn Building, 5600 Fishers Lane, Rockville, Maryland, 20857. (301) 443–5363. January 15, 2002. <<http://lhncbc.nlm.nih.gov/apdb/phsHistory>> (December 14, 2002).

### SEE ALSO

- CDC (United States Centers for Disease Control and Prevention)*
- NIH (National Institutes of Health)*
- Health and Human Services Department, United States*

---

## Pueblo Incident

---

### ■ ADRIENNE WILMOTH LERNER

The *Pueblo* incident involved the 1968 seizure and hijacking of the USS *Pueblo* by North Korean military forces. The *Pueblo*, a naval intelligence ship, was conducting offshore surveillance of North Korean radar and radio installations when it was overtaken by the North Korean fleet. Following seizure of the ship, diplomatic tensions between the United States and North Korea heightened. North Korean officials claimed that the vessel, and the United States government, had been warned about conducting espionage activities in the region. In contrast, United States officials claimed that the *Pueblo* was seized in international waters, without provocation. The crew of the *Pueblo*

was detained in North Korea for nearly a year before their release was negotiated.

In 1967, the Navy refurbished one of its aging cargo ships, transforming it into a remote intelligence collection vessel. The old hull provided sufficient camouflage for the classified communications and radar locator systems on-board. Because the projected missions for the ship were considered low risk, the *Pueblo* was outfitted with only minimal defensive weapons. The U.S. Fifth Air Force stationed in Fuchu, Japan, was designated to aid the *Pueblo* if necessary, but no specific teams were reserved from daily operations or put on alert.

The *Pueblo*, commanded by U.S. Navy Commander Lloyd. M. "Pete" Bucher, was assigned a new, and relatively inexperienced crew. The crew reported to San Diego for training maneuvers, and then departed for Pearl Harbor, Hawaii. Upon its arrival in Pearl Harbor, the *Pueblo* needed significant repairs to its steering engine.

***Pueblo's* mission CBIAC operations.** The ultimate mission of the *Pueblo* crew remained classified until official mission orders were given to the crew after departing Pearl Harbor in late November, 1967. The ship arrived in Yokosuka, Japan, where further adjustments to onboard systems were made, and soon after departed on January 11, 1968.

Bound for international waters off the eastern coastline of North Korea, the *Pueblo's* stated mission was oceanographic research. However, the ship was part of a covert naval intelligence mission code named Operation Clickbeetle. The ship was charged with conducting a detailed survey of increasing North Korean naval activity, including assessing its potential fleet strength. Operation Clickbeetle further used the sophisticated equipment below decks on the *Pueblo* to intercept Soviet-North Korean communications, and locate radar and radio stations inland. Naval intelligence, in conjunction with the National Security Agency and the Naval Security Group Command, devised Operation Clickbeetle as part of a larger Cold War-era monitoring and espionage project intended to garner information about the influence of the Soviet Union on its satellite nations.

The *Pueblo* was assigned three operational areas in which to work, code named Pluto, Venus, and Mars. The first two areas, Pluto and Venus, off the northeast coast of the Korean Peninsula, yielded very little information. The *Pueblo* therefore moved to its final area further south, Mars, ahead of schedule. While in transit, the *Pueblo* crossed paths with a Soviet-made North Korean subchaser vessel. Since the *Pueblo* was instructed to maintain radio silence, it did not report the encounter to its support team in Japan. Furthermore, the *Pueblo* was 30 miles from the coastline, well into established international waters. After arriving in Op Area Mars on January 22, the *Pueblo* was again approached by two North Korean vessels. The two boats, apparent fishing trawlers, circled the *Pueblo* at close range. Sensing the foreign vessels may have been



The USS *Pueblo*, shown underway at sea, was captured in 1968 by North Korean patrol boats with 83 men aboard, who smashed intelligence-gathering equipment and burned sensitive documents just moments before the vessel was boarded by North Koreans. AP/WIDE WORLD PHOTOS.

sent to conduct reconnaissance on the *Pueblo*, Commander Bucher sent a civilian team to the ship's deck to conduct oceanographic research, maintaining the ship's cover. After the North Korean vessels left the area, the communications room aboard the *Pueblo* began intercepting increasing electronic communications between the ships and on shore stations. The *Pueblo* broke communications silence and notified Naval command of the situation.

Naval command received the message sent by the *Pueblo* fourteen hours later. During that time, a special unit of North Korean soldiers, dressed as South Korean military personnel, crossed the internationally established Demilitarized Zone into South Korea. The unit traveled to Seoul on a mission to attack South Korean government buildings and potentially assassinate the South Korean President. The North Korean saboteurs were discovered within miles of the presidential palace, and later executed. The incident brought the two nations again to the brink of war, and heightened tensions between the United States

and the Soviet Union. United States Naval Command decided that the *Pueblo* did not need to be informed about the event, and that the vessel was safe in international waters. They advised the ship merely to relocate an additional five nautical miles from the coastline, a full 15 nautical miles into international waters.

On January 23, a small fleet of North Korean ships approached the *Pueblo*. Commander Bucher and the crew noticed that the vessels were staffed at battle stations. The *Pueblo* intercepted transmissions revealing that the intent of the ships was to board the *Pueblo*, overtake the crew, and pilot the ship to North Korea. The crew was put on alert, and the *Pueblo* made way further into international waters. A North Korean subchaser signaled four nearby torpedo boats, and the fleet encircled the *Pueblo*. A North Korean military boarding party attempted to come aside the *Pueblo*, but the ship took evasive measures. Soon after, one of the North Korean vessels fired upon the *Pueblo*. Commander Bucher ordered all of the classified

documents, information, and devices on the ship be destroyed. The ship then radioed Navy Pacific Fleet Command requesting emergency aid from military installations in Japan.

**Hijack of the ship and crew.** Another group of North Korean military attempted to board the *Pueblo*, this time sweeping the deck with heavy fire. At this time, fireman Duane Hodges, was killed while fending off the group attempting to board the ship. The United States vessel again attempted evasive maneuvers, but the ship was too slow and heavily out gunned by the surrounding four torpedo boats, two subchasers, and two Soviet-made MiG aircraft. The *Pueblo* stopped in the water and heeded instructions to follow the lead North Korean boat. Commander Bucher ordered the vessel to travel at its slowest speed to give the men time to destroy the classified equipment onboard. The *Pueblo* then steamed full speed and again tried to evade the fleet. The North Korean forces fired explosive shells onto the deck of the ship, injuring several crewmembers. The *Pueblo* again stopped, and the ranking officer of the North Korean vessels ordered the boarding party to seize control of the U.S. ship. A North Korean fisherman, working for the military, then piloted the *Pueblo*, at full speed, into the harbor at Wonsan. The crewmembers of the *Pueblo* were tied up and corralled on the forward well deck, before being transferred to their quarters.

After the arrival of the ship into North Korean port, the crew and command of the *Pueblo* were paraded in front of national media as grand propaganda and then shipped to a series of secret detention facilities. Their imprisonment began in a sparse, remote prison on January 24, 1968. Over the course of a year, the crew suffered mental and physical torture at the hands of their captors. Severe beatings were routine, and the crew received inadequate food and medical care. While United States diplomatic envoys tried to secure their release, the North Korean government provided staged photographs of the prisoners playing sports and enjoying leisure activities. Several crewmembers displayed their middle finger in the photographs to indicate that the photos were merely staged propaganda. When North Korean officials realized the gesture's meaning, the crew was again beaten.

Official diplomatic negotiations failed to secure the release of the *Pueblo* crew. Only after Commander Bucher and the other officers of the ship capitulated under severe duress to demands to sign a confession of wrongdoing and espionage activities did the North Korean government agree to discuss the release of their American prisoners. Members of the Military Armistice Committee met twenty eight times after the capture of the *Pueblo*. The United States and North Korean diplomats fought over the release of the ship's crew for nearly eleven months before the U.S. diplomatic mission agreed to admit guilt for the incident and sign a statement similar to that signed by the *Pueblo* officers. Before the official signing of the North Korean drafted document, diplomatic representative Major

General Gilbert Woodward issued a statement to the United States government disavowing the admission of culpability and dismissing the North Korean treaty. He further stated that the United States does not officially apologize for any past actions in the incident and that the North Korean document would be signed for no other purpose than to insure the release of the *Pueblo* crew. The command and crew of the *Pueblo* was officially released on December 28, 1968, after nearly a year of captivity.

Although the North Korean government finally capitulated to the release of the crew of *Pueblo*, they refused to return the ship itself. The ship was evaluated and photographed by North Korean military intelligence, as well as Soviet officials. Because much of the classified equipment onboard had been destroyed by the crew during the hijacking, the North Koreans and Soviets gained little information about United States remote intelligence gathering equipment and operations. The *Pueblo* remained in Wonsan harbor for nearly three decades, serving as a propaganda piece and museum. In 1998, the North Korean government relocated the *Pueblo*. The boat was towed to the west coast of North Korea, and remains a propagandistic museum.

The crew of the *Pueblo* received little recognition for their actions in preventing the transfer of classified material onboard the ship to enemy powers, or for their time in captivity. Following their release, crewmembers received the Purple Heart for wounds received in action. The *Pueblo*'s officers endured a series of inquiries and hearings regarding their negotiations with their North Korean captors. At one time, naval officials considered court marshal for Commander Bucher and several other officers for signing the North Korean written confession of American wrongdoing. However, no member of the command or crew ever received disciplinary action. The lack of recognition for their service, and the numerous conduct inquiries, drew sharp criticism from the veterans of Operation Clickbeetle and the public. At the end of the Vietnam War, a series of retrospective stories in a national magazine drew attention to the *Pueblo* Incident and the plight of the *Pueblo* crew. The Navy then granted several more awards to various crewmembers, including a posthumous award of the Silver Star to Duane Hodges. In 1990, in accordance with a special act of Congress, the crew and command of the *Pueblo* was finally granted Prisoner of War (POW) status for their time in captivity.

The *Pueblo* was the first United States Navy vessel commandeered since the American Civil War. It was the only ship to surrender to hostile forces, other than those with whom the United States was at war, since the *Chesapeake* in 1807.

#### ■ FURTHER READING:

##### BOOKS:

Bucher, Loyd M. *My Story*. New York: Doubleday, 1970.

Lerner, Mitchell B. *The Pueblo Incident: A Spy Ship and the Failure of American Foreign Policy*. Lawrence, KS: University Press of Kansas, 2002.

#### SEE ALSO

*Korean War*  
*North Korea, Intelligence and Security*  
*Radio, Direction Finding Equipment*  
*Vietnam War*

## Purple Machine

■ ADRIENNE WILMOTH LERNER

The Purple Machine was an Allied codename for one of several Japanese cipher machines used during World War Two. The nickname Purple Machine was derived from the

name of the code the machine produced. The first intercepted Japanese code was dubbed “Orange” by American code breakers. As the codes increased in sophistication and difficulty to decipher, cryptologists referred to the various cipher permutations with the names of colors. “Purple” was the most difficult Japanese code to break, and was used to transmit diplomatic messages from 1939 until 1945.

The mechanics of the Purple Machine were similar to other Axis encoding machines, such as the German Enigma cipher. The Purple Machine used the twenty-six-letter Latin alphabet, programmed into a pegboard with corresponding wires that governed cipher wheels, or rotors. The machine itself consisted of a typewriter joined by wires and a circuit board to a series of four rotors that shifted the type in various permutations on a second typewriter to produce coded text. The coded text was sent by wire, preceded by a series of coded numbers that revealed the permutations used to create the code. With the setting adjusted as specified, the encoded text could



Two intelligence analysts work at Purple code deciphering machines at the headquarters of the U.S. Army cryptanalysis service in Arlington, Virginia, in 1944. AP/WIDE WORLD PHOTOS.

then be deciphered by again running it through the machine.

While many pre-war Japanese codes were broken mathematically with pen and paper, effectively deciphering Purple required constructing an identical cipher machine. American cryptologist William Friedman built a replica of the Purple Machine, based on intelligence information, in 1939. When the machine became operational, American code breakers were able to monitor most Japanese diplomatic messages that used the Purple code.

While breaking Purple gave U.S. intelligence services a great deal of information regarding diplomatic activities and strategies, it seldom yielded specific information regarding naval actions or fleet positions. The Japanese used a separate code for military operations, fleet positions, and troop deployments. In the months prior to the bombing of Pearl Harbor in 1941, Purple Machine intercepts indicated that the Japanese were planning an attack, but the messages did not mention Hawaii, Pearl Harbor, or a date for such an attack. However, the Japanese government did use Purple to deliver their ultimatum the day before the attack. Cryptologists decoded the series of fourteen messages between the Japanese government and their embassy in Washington, D.C., and passed the messages along to the Department of the Navy. A further intercept in the early hours of December 7, 1941, indicated that the Japanese fleet was poised and awaiting the order to attack. No action was taken on the information in the intercepts, and the U.S. Pacific fleet was bombed in port at Pearl Harbor later that day.

After Pearl Harbor, deciphered Purple Machine intercepts yielded substantial intelligence information for the United States. Paired with deciphered Japanese Navy dispatches that used another broken code, Purple Machine intercepts helped the United States to victory at the battle of Midway. In the weeks before the battle, code breakers discovered a series of messages from Tokyo to Japanese

diplomats and Navy officers that discussed battle strategy in the Pacific. Some of the communications yielded fleet positions. Decoded Purple messages also allowed Allied planes to track and shoot down a military flight carrying Japanese Admiral Isoroku Yamamoto.

Breaking Purple Machine code even aided the Allied effort on the European front. A long series of dispatches between Japanese diplomats in Germany and the Japanese command in Tokyo discussed meetings with Hitler and revealed information about German defenses in occupied France. This information helped Allied forces prepare for the D-Day invasion of the continent.

The Japanese remained confident throughout the war that the Purple Machine and its code remained unbroken by the Allies, and continued to use the code even in the weeks immediately following their surrender in 1945. In United States hearings regarding intelligence, military, and political oversights in the days prior to Pearl Harbor, the government revealed that it broke the Purple code before the outbreak of the war. It was the first time former Japanese forces heard that the secrecy of the Purple Machine had been long compromised.

#### ■ FURTHER READING:

##### BOOKS:

Clark, Ronald William. *The Man Who Broke Purple: The Life of Colonel William F. Friedman, Who Deciphered the Japanese Code in World War II*. New York: Little & Brown, 1977.

Budiansky, Stephen. *Battle of Wits: The Complete Story of Codebreaking in World War II*. New York: Touchstone Books, 2002.

##### SEE ALSO

*World War II*  
*World War II, United States Breaking of Japanese Naval Codes*



## Quadratic Sieves.

SEE *Cryptography and Number Theory*.

---

## Quantum Physics: Applications to Espionage, Intelligence, and Security Issues

---

■ K. LEE LERNER/LARRY GILMAN

Quantum physics, which has been called “the science of the very small,” is essential to the design of modern microelectronics. Without quantum physics it would not be possible to design the microscopic structures that make today’s digital circuits possible. Such circuits, in turn, are essential to the conduct of all kinds of modern espionage, warfare, and security operations. The further application of quantum physics to computing and communications is at present being systematically researched by many groups, including the U.S. Quantum Information Science and Technology (QIST) Program of the Defense Advanced Research Projects Agency (DARPA). DARPA has historically funded the development of such fundamental advances in electronics as the microchip.

### Limitations of Conventional Electronics

Ordinary circuit components obey the laws of classical physics; that is, their behavior is predictable and single-valued. An integrated-circuit memory cell is either ON or OFF, never both at once. There is no upper limit on how large a device exhibiting such behavior can be; one could

build a computer out of stars and planets, if one had the means to move them about. However, the laws of quantum physics place strict limits on how small a device can be and still behave classically. Quantum physics tells chip designers how small they can make their transistors and other circuit components and still obtain classical, causal behavior from them.

However, quantum effects (those physical laws that dominate the behavior of matter at the subatomic level) are not only an obstacle to infinite miniaturization, they can be exploited to produce devices that have no parallel in the macroscopic world, the world of large objects. An early example of such a device is the tunnel diode (invented in 1958), an electronic device that takes advantage of the fact that an individual subatomic particle can appear randomly on the far side of an otherwise insurmountable barrier (i.e., “tunnel” through the barrier). Despite a few oddities such as the tunnel diode, however, quantum phenomena have for decades been perceived by designers of computers and communications systems more as a limiting factor on conventional device size than as an invitation to build novel devices.

Since the 1990s, physicists have realized that quantum phenomena open the door to powerful new techniques in computing and communications. In particular, they are hoping to exploit the phenomenon of quantum “entanglement” to produce superfast computers, unbreakable cryptographic systems, and error-free transmission of information. All of these advances, when they become available in working devices, will have many uses in both the civil and military sectors.

The concepts of quantum entanglement and quantum information are basic to the development of new quantum computing, cryptography, and communications technologies, and are reviewed separately below.

### Entanglement

Individual subatomic particles, such as photons, do not exist in single, well-defined states like on-off light switches.

Rather, they exist as a superposition of states. Experiments show, for example, that prior to observation (i.e., definitive interaction with a large-scale system) a photon can actually have more than one polarization at once and be in more than one place at once.

Not only can individual particles exist in superposed or ambiguous states prior to observation, but the superposed states of pairs, triplets, or larger groups of particles can be related to each other by means of entanglement. Entanglement arises because the superposed states of particles that have interacted directly retain a definite, permanent relationship even after the particles have separated. Two entangled photons, for example, may be sent to two different detectors, A and B. Individually the photons do not, while in transit, have definite polarizations. When the polarization of one of the photons is collapsed to a definite value by measurement at detector A, however, photon, bound for detector B, instantly takes on the opposite polarization. There is no delay; the effect is truly instantaneous.

Despite appearances, this does not offer a means of faster-than-light communication (which would contradict the special theory of relativity); there is, in principle, no way to control what polarization detector A observes. The observed value at detector A is random, and the value that is instantly imposed on the photon bound for detector B is also random. There is thus no way for A to signal to B by using the instantaneous relationship between the entangled photons. However, entanglement is still useful. Transmission of an identical string of random bits to two receivers is important in cryptography, and using a stream of entangled photons for transmitting that bitstream has the valuable property that it cannot be eavesdropped upon, as quantum physics declares that any effort to interfere with (i.e., measure) either entangled photon en route will be detectable by the intended receivers. Nonquantum or classical communications links cannot give this absolute privacy guarantee. Transmission of entangled photon pairs over tens of kilometers of optical fiber has recently been demonstrated, bringing quantum cryptography closer to practical realization.

Entangled photons can also be used to achieve what is termed superdense coding or quantum dense coding—the transmission of multiple bits of classical information through the transmission of a smaller number of qubits (entangled photons). Another application of entanglement is quantum teleportation, discussed further below.

## Quantum Information and its Implications for Communications and Computing

The quantum phenomena of superposition and entanglement have important implications for computing and communications, even apart from cryptography. In classical information theory, the minimum unit of information is a

bit (short for “binary digit,” since a bit is usually, though arbitrarily, symbolized as a 1 or 0); in quantum information theory, the minimum unit of information is the quantum bit or qubit (pronounced CUE-bit). One qubit is the amount of quantum information stored by a microscopic system (e.g., photon) that exists in a superposed pair of states. Quantum computation applies logical operations to qubits, much as classical computation applies Boolean logical operations to bits. The advantage of quantum computation arises from the superposition property of quantum systems:  $L$  qubits (e.g., isolated atoms) can, through superposition, contain the equivalent of  $2^L$  bits, and quantum-logical operations can be performed simultaneously on all those bits. The result, potentially, is massive parallelism with corresponding speedup of certain calculations. One important class of calculations that would be greatly speeded by a quantum computer is the factorization of a large integer  $N$ . Factorization is the discovery, given  $N$ , of two numbers  $x$  and  $y$  such that  $x \times y = N$ . For large  $N$  this is a time-consuming calculation, and it is on this difficulty that many cryptosystems (e.g., public-key cryptography) depend. When quantum computers are built, such cryptosystems will quickly become worthless, for the factorization problem will have become manageable even for very large  $N$ .

Many nuts-and-bolts obstacles remain, however, in the construction of a full-scale quantum computer. One challenge is the accurate transmission of quantum information—qubits, held in superposed quantum states—from one place to another within a quantum computer or between one quantum computer and another. Quantum teleportation may provide a practical answer to this problem. Quantum teleportation allows the perfect recreation of a quantum system at the far end of a transmission channel. In this technique, one member of an entangled photon pair is combined at a transmitter with the quantum system to be teleported—a photon, other particle, or even a collection of particles—in such a way that bits of classical information (1s and 0s) are produced that characterize the system to be teleported. Both the entangled photon and the system to be teleported are destroyed by this process; that is, they no longer exist as a superposition of quantum states, but are measured as having definite, unique values. The classical information (bits) derived by the transmitter from its measurements is sent in conjunction with the remaining member of the entangled photon pair to a distant receiver. The receiver can re-create or “resurrect” the original quantum system with all its superpositional ambiguity (qubit content) intact, just as if it had never been measured (destroyed) by the transmitting system. Because quantum physics declares that systems with identical quantum-mechanical descriptions are not only *similar* but are *the same*—have no individuality, cannot be distinguished from each other—the “resurrected” system in effect *is* the original system: that is, the original system has been teleported from the transmitter to the receiver, including whatever quantum information it contains. (Strictly speaking, every quantum system—e.g.,



photon—contains an infinite amount of information; most of this, however, is in principle unextractable.) Quantum teleportation has already been demonstrated at kilometer distances for single-particle systems, and may eventually be used to communicate quantum information without error from one part of a quantum computer to another. However, it will never be practical to teleport large systems of particles such as human beings; the number of bits to be transmitted would be prohibitively large.

#### ■ FURTHER READING:

##### PERIODICALS:

Bennett, Charles H., and Peter W. Shor. "Privacy in a Quantum World." *Science* 284 (April 30, 1999):747–748.

Bennett, Charles H., and David P. DiVincenzo. "Quantum information and computation." *Nature* 404 (March 16, 2000): 247–255.

Taubes, Gary. "Quantum Mechanics: To Send Data, Physicists Resort to Quantum Voodoo." *Science* 274 (Oct. 25, 1996): 504–505.

##### SEE ALSO

*Nanotechnology*

## Quarantine.

SEE *Communicable Diseases, Isolation, and Quarantine.*

*This page intentionally left blank*

E N C Y C L O P E D I A   O F  
**Espionage, Intelligence, and Security**



E N C Y C L O P E D I A O F

# Espionage, Intelligence, and Security

*This page intentionally left blank*

E N C Y C L O P E D I A O F  
Espionage, Intelligence, and Security

K. LEE LERNER AND BRENDA WILMOTH LERNER, EDITORS

v o l u m e  
1 3 1  
R - Z  
I N D E X



THOMSON  
—★—™  
GALE



## Encyclopedia of Espionage, Intelligence, and Security

K. Lee Lerner and Brenda Wilmoth Lerner, editors

**Project Editor**  
Stephen Cusack

**Editorial**  
Erin Bealmear, Joann Cerrito, Jim Craddock,  
Miranda Ferrara, Kristin Hart, Melissa Hill,  
Carol Schwartz, Christine Tomassini, Michael  
J. Tyrkus, Peter Gareffa

**Permissions**  
Lori Hines

**Imaging and Multimedia**  
Dean Dauphinais, Leitha Etheridge-Sims, Mary  
K. Grimes, Lezlie Light, Luke Rademacher

**Product Design**  
Kate Scheible

**Manufacturing**  
Rhonda Williams

© 2004 by Gale. Gale is an imprint of The  
Gale Group, Inc., a division of Thomson  
Learning, Inc.

Gale and Design™ and Thomson Learning™  
are trademarks used herein under license.

*For more information, contact*  
The Gale Group, Inc.  
27500 Drake Rd.  
Farmington Hills, MI 48331-3535  
Or you can visit our Internet site at  
<http://www.gale.com>

### ALL RIGHTS RESERVED

No part of this work covered by the copyright  
hereon may be reproduced or used in  
any form or by any means—graphic,  
electronic, or mechanical, including  
photocopying, recording, taping, Web  
distribution, or information storage retrieval  
systems—without the written permission of  
the publisher.

For permission to use material from this  
product, submit your request via Web at  
<http://www.gale-edit.com/permissions>, or you  
may download our Permissions Request form  
and submit your request by fax or mail to:

*Permissions Department*  
The Gale Group, Inc.  
27500 Drake Rd.  
Farmington Hills, MI 48331-3535  
Permissions Hotline:  
248-699-8006 or 800-877-4253, ext. 8006  
Fax: 248-699-8074 or 800-762-4058

### Cover Photos

Volume 1: Ethel and Julius Rosenberg  
following arraignment on charges of  
espionage, August 23, 1950.  
©Bettmann/Corbis

Volume 2: SR-71 Blackbird, c. 1991. ©Corbis

Volume 3: Clean-up crews scour the American  
Media Inc. building in Boca Raton, Florida,  
after the discovery of anthrax spores, October  
9, 2001. AP/Wide World Photos.

While every effort has been made to  
ensure the reliability of the information  
presented in this publication, The Gale Group,  
Inc. does not guarantee the accuracy of  
the data contained herein. The Gale Group,  
Inc. accepts no payment for listing; and  
inclusion in the publication of any  
organization, agency, institution, publication,  
service, or individual does not imply  
endorsement of the editors or publisher.  
Errors brought to the attention of the  
publisher and verified to the satisfaction of  
the publisher will be corrected in future  
editions.

### Library of Congress Cataloging-in-Publication Data

Encyclopedia of espionage, intelligence, and security / K. Lee Lerner  
and Brenda Wilmoth Lerner, editors.  
p. cm.

Includes bibliographical references and index.

ISBN 0-7876-7546-6 (set : hardcover : alk. paper) — ISBN  
0-7876-7686-1 (v. 1) — ISBN 0-7876-7687-X (v. 2) — ISBN 0-7876-7688-8  
(v. 3)

1. Espionage—Encyclopedias. 2. Intelligence service—Encyclopedias.  
3. Security systems—Encyclopedias. I. Lerner, K. Lee. II. Lerner,  
Brenda Wilmoth.  
JF1525.I6E63 2004  
327.12'03—dc21

2003011097

This title is available as an e-book.  
ISBN 0-7876-7762-0

Contact your Gale sales representative for ordering information.

Printed in the United States of America  
10 9 8 7 6 5 4 3 2 1

# Contents

INTRODUCTION	VII
ADVISORS AND CONTRIBUTORS	XI
LIST OF ENTRIES	XIII
The Encyclopedia of Espionage, Intelligence, and Security	
	1
GLOSSARY	289
CHRONOLOGY	317
SOURCES	353
INDEX	403



*This page intentionally left blank*

# Introduction

In composing *The Encyclopedia of Espionage, Intelligence, and Security (EEIS)*, our goal was to shape a modern encyclopedia offering immediate value to our intended readers by emphasizing matters of espionage, intelligence, and security most frequently in the news.

*EEIS* is not intended as a classical “spy book,” filled with tales of daring operations. Instead, within a framework of historical overviews, *EEIS* emphasizes the scientific foundations, applications of technology, and organizational structure of modern espionage, intelligence, and security. High school and early undergraduate students can use this book to expand upon their developing awareness of the fundamentals of science, mathematics, and government as they begin the serious study of contemporary issues.

*EEIS* is also intended to serve more advanced readers as a valuable quick reference and as a foundation for advanced study of current events.

*EEIS* devotes an extensive number of articles to agencies and strategies involved in emerging concepts of homeland security in the United States. Faced with a daunting amount of information provided by agencies, organizations, and institutes seeking to put their best foot forward, we have attempted to allocate space to the topics comprising *EEIS* based upon their relevance to some unique facet of espionage, intelligence, or security—especially with regard to science and technology issues—as opposed to awarding space related to power of the agency or availability of material.

A fundamental understanding of science allows citizens to discern hype and disregard hysteria, especially with regard to privacy issues. Spy satellites powerful enough to read the details of license plates do so at peril of missing events a few steps away. With regard to electronic intercepts, the capability to identify what to carefully examine—often a decision driven by mathematical analysis—has become as essential as the capacity to gather the intelligence itself. Somewhere between the scrutiny of

Big Brother and the deliberately blind eye lie the shadows into which terrorists often slip.

With an emphasis on the realistic possibilities and limitations of science, we hope that *EEIS* finds a useful and unique place on the reference shelf.

It seems inevitable that within the first half of the twenty-first century, biological weapons may eclipse nuclear and chemical weapons in terms of potential threats to civilization. Because informed and reasoned public policy debates on issues of biological warfare and bioterrorism can only take place when there is a fundamental understanding of the science underpinning competing arguments, *EEIS* places special emphasis on the multifaceted influence and applications of the biological sciences and emerging biometric technologies. Future generations of effective intelligence and law enforcement officers seeking to thwart the threats posed by tyrants, terrorists, and the technologies of mass destruction might be required to be as knowledgeable in the terminology of epidemiology as they are with the tradecraft of espionage.

Knowledge is power. In a time where news can overwhelm and in fact, too easily mingle with opinion, it is our hope that *EEIS* will provide readers with greater insight to measure vulnerability and risks, and correspondingly, an increased ability to make informed judgments concerning the potential benefits and costs of espionage, intelligence, and security matters.

■ K. LEE LERNER & BRENDA WILMOTH LERNER, EDITORS  
CORNWALL, U.K.  
MAY, 2003

## How to Use the Book

The *Encyclopedia of Espionage, Intelligence, and Security* was not intended to contain a compendium of weapons systems. Although *EEIS* carries brief overviews of specifically selected systems commonly used in modern intelligence operations, readers interested in detailed information regarding weapons systems are recommended

to *Jane's Strategic Weapon Systems*, or *Jane's Defense Equipment Library*.

Although *EEIS* contains overview of significant historical periods and events, for those readers interested in additional information regarding the history of espionage operations and biographies of intelligence personnel, the editors recommend Jeffrey T. Richelson's *A Century of Spies: Intelligence in the Twentieth Century* (Oxford University Press, 1995), Vincent Buranelli and Nan Buranelli's *Spy/Counterspy: An Encyclopedia of Espionage* (New York: McGraw-Hill, 1982), and Allen Dulles', *The Craft of Intelligence* (New York: Harper & Row, 1963).

The articles in *EEIS* are meant to be understandable by anyone with a curiosity about topics in espionage, intelligence, and security matters, and this first edition of the book has been designed with ready reference in mind:

- Entries are arranged alphabetically. In an effort to facilitate easy use of this encyclopedia, and to attempt order in a chaotic universe of names and acronyms the editors have adopted a "common use" approach. Where an agency, organization, or program is known best by its acronym, the entry related to that organization will be listed by the acronym (e.g. FEMA is used instead of Federal Emergency Management Agency). To facilitate use, the editors have included a number of "jumps" or cross-referenced titles that will guide readers to desired entries.
- To avoid a log jam of terms starting with "Federal" and "United States," titles were broken to most accurately reflect the content emphasized or subject of agency authority.
- "**See Also**" references at the end of entries alert the readers to related entries not specifically mentioned in the body of the text that may provide additional or interesting resource material.
- An extensive **Glossary** of terms and acronyms is included to help the reader navigate the technical information found in *EEIS*.
- The **Chronology** includes significant events related to the content of the encyclopedia. Often accompanied by brief explanations, the most current entries date represent events that occurred just as *EEIS* went to press.
- A **Sources** section lists the most worthwhile print material and web sites we encountered in the compilation of this volume. It is there for the inspired reader who wants more information on the people and discoveries covered in this volume.
- A comprehensive general **Index** guides the reader to topics and persons mentioned in the book. Bolded page references refer the reader to the term's full entry.
- The editors and authors have attempted to explain scientific concepts clearly and simply, without sacrificing fundamental accuracy. Accordingly, an advanced understanding of physics, chemistry, or biochemistry is not assumed or required. Students and other readers should not, for example, be intimidated or deterred by the complex names of biochemical

molecules—where necessary for complete understanding, sufficient information regarding scientific terms is provided.

- To the greatest extent possible we have attempted to use Arabic names instead of their Latinized versions. Where required for clarity we have included Latinized names in parentheses after the Arabic version. Alas, we could not retain some diacritical marks (e.g. bars over vowels, dots under consonants). Because there is no generally accepted rule or consensus regarding the format of translated Arabic names, we have adopted the straightforward, and we hope sensitive, policy of using names as they are used or cited in their region of origin.
- *EEIS* relies on open source material and no classified or potentially dangerous information is included. Articles have been specifically edited to remove potential "how to" information. All articles have been prepared and reviewed by experts who were tasked with ensuring accuracy, appropriateness, and accessibility of language.
- With regard to entries regarding terrorist organizations, *EEIS* faced a serious dilemma. For obvious reasons, it was difficult to obtain balanced, impartial, and independently verifiable information regarding these organizations, nor could *EEIS* swell to incorporate lengthy scholarly analysis and counter-analysis of these organizations without losing focus on science and technology issues. As a compromise intended to serve students and readers seeking initial reference materials related to organizations often in the news, *EEIS* incorporates a series of supplemental articles to convey the information contained in the U.S. Department of State annual report to Congress titled, *Patterns of Global Terrorism*, 2001. These articles contain the language, assertions of fact, and views of the U.S. Department of State. Readers are encouraged to seek additional information from current U.S. Department of State resources and independent non-governmental scholarly publications that deal with the myriad of issues surrounding the nature and activities of alleged terrorist organizations. A number of governmental and non-governmental publications that deal with these issues are cited in the bibliographic sources section located near the index.

Key *EEIS* articles are signed by their authors. Brief entries were compiled by experienced researchers and reviewed by experts. In the spirit of numerous independent scientific watchdog groups, during the preparation of *EEIS* no contributors held a declared affiliation with any intelligence or security organization. This editorial policy not only allowed a positive vetting of contributors, but also assured an independence of perspective and an emphasis on the fundamentals of science as opposed to unconfirmable "insider" information.

When the only verifiable or attributable source of information for an entry comes from documents or information provided by a governmental organization (e.g., the U.S. Department of State), the editors endeavored to carefully note when the language used and perspective offered was that of the governmental organization.

Although some research contributors requested anonymity, no pseudonyms are used herein.

## Acknowledgments

The editors wish to thank Herbert Romerstein, former USIA Soviet Disinformation Officer and Coordinator of Programs to Counter Soviet Active Measures, United States Information Agency, for his assistance in compiling selected articles.

The editors wish to thank Lee Wilmoth Lerner for his assistance in compiling technical engineering data for inclusion in *EEIS*.

The editors acknowledge the assistance of the members of the Federation of American Scientists for the provision of reports and materials used in the preparation of selected articles.

Although certainly not on the scale of the challenge to provide security for a nation with approximately 85 deep-draft ports, 600,000 bridges, 55,000 independent water treatment systems, 100 nuclear power plants, and countless miles of tunnels, pipelines, and electrical and communications infrastructure, the task of incorporating changes brought on by creation of the Department of Homeland Security—and the most massive reorganization of the United States government since World War II—as this book went to press provided a unique challenge to *EEIS*

writers and advisors. The editors appreciate their dedication and willingness to scrap copy, roll up their sleeves, and tackle anew the smorgasbord of name and terminology changes.

As publishing deadlines loomed, *EEIS* was also well served by a research staff dedicated to incorporating the latest relevant events—especially information related to the search for weapons of mass destruction—that took place during war in Iraq in March and April of 2003.

*EEIS* advisors, researchers, and writers tenaciously attempted to incorporate the most current information available as *EEIS* went to press. The editors pass any credit or marks for success in that effort, and reserve for themselves full responsibility for omissions.

The editors gratefully acknowledge the assistance of many at St. James Press for their help in preparing *The Encyclopedia of Espionage, Intelligence, and Security*. The editors extend thanks to Mr. Peter Gareffa and Ms. Meggin Condino for their faith in this project. Most directly, the editors wish to acknowledge and thank the project editor, Mr. Stephen Cusack, for his talented oversight and for his tireless quest for secure engaging pictures for *EEIS*.

The editors lovingly dedicate this book to the memory of Wallace Schaffer, Jr., HM3, USNR, who died on January 8, 1968, in Thua Thien (Hue) Province, Vietnam.

“A small rock holds back a great wave.”—Homer, *The Odyssey*.

*This page intentionally left blank*

## Advisors and Contributors

**Julie Berwald, Ph.D.**

*Geophysicist, writer on marine science, environmental biology, and issues in geophysics.*  
Austin, Texas

**Robert G. Best, Ph.D.**

*Clinical cytogeneticist and medical geneticist who has written on a range of bioscience issues*  
Director, Division of Genetics  
University of South Carolina School of Medicine

**Tim Borden, Ph.D.**

*Doctorate in History from Indiana University, and is an inspector with the U.S. Bureau of Customs and Border Protection*  
Toledo, Ohio

**Brian Cobb, Ph.D.**

*Bioscience writer, researcher*  
Institute for Molecular and Human Genetics  
Georgetown University, Washington, D.C.

**Cecilia Colomé, Ph.D.**

*Astrophysicist, translator, and science writer*  
Austin, Texas

**Laurie Duncan, Ph.D.**

*Geologist, science writer, and researcher*  
Austin, Texas

**William J. Engle, P.E.**

*Writer on contemporary geophysics issues and the impacts of science and technology on history*  
Exxon-Mobil Oil Corporation (Rt.) New Orleans, Louisiana

**Antonio Farina, M.D., Ph.D.**

*Physician, researcher, and writer on medical science issues*  
Assistant Professor, University of Bologna, Italy

**Christopher T. Fisher, Ph.D.**

*Assistant Professor, Department of African American Studies and the Department of History*  
The College of New Jersey, Ewing, New Jersey

**Larry Gilman, Ph.D.**

*Electrical engineer and science writer*  
Sharon, Vermont

**William Haneberg, Ph.D.**

*Former research scientist and professor, now an independent consulting geologist and science writer*  
Portland, Oregon

**Brian D. Hoyle, Ph.D.**

*Science writer and Chief Microbiologist, Government of New Brunswick from 1993 to 1997*  
Nova Scotia, Canada

**Joseph Patterson Hyder**

*Writer on the historical impacts of science and technology*  
University of Tennessee College of Law, Knoxville, Tennessee

**Alexandr Ioffe, Ph.D.**

*Writer on the history of science and researcher with the Geological Institute of Russian Academy of Sciences in Moscow*  
Russian Academy of Sciences, Moscow

**Judson Knight**

*Science writer, researcher, and editor*  
Knight Agency Research Services, Atlanta, Georgia

**Michael Lambert, Ph.D.**

*Researcher at the Great Plains/Rocky Mountain Hazardous Substance Research Center and at the U.S. Naval Research Laboratory*  
Manhattan, Kansas

**Adrienne Wilmoth Lerner**

*Writer of various articles on the history of science, archaeology, and the evolution of security-related law*  
University of Tennessee College of Law, Knoxville, Tennessee

**Agnes Lichanska, Ph.D.**

*Science writer who has conducted research at the Department of Medical Genetics and Ophthalmology at Queen's University of Belfast (Northern Ireland)*

University of Queensland, Brisbane, Australia

**Eric v.d. Luft, Ph.D., M.L.S.**

*Writer on cultural, scientific, and intellectual history, and philosophy*

Curator of Historical Collections  
SUNY Upstate Medical University, Syracuse, New York

**Martin Manning**

*Served on the Economic Security Team, Office of International Information Programs, U.S. Department of State*

Bureau of Public Diplomacy  
U.S. Department of State, Washington, D.C.

**Kelli Miller**

*Served as news writer and producer for Inside Science TV News at the American Institute of Physics (AIP) and as executive producer of Discoveries & Breakthroughs Inside Science*

Atlanta, Georgia

**Caryn E. Neumann**

*Instructor and doctoral candidate in the Department of History at Ohio State University*

Columbus, Ohio

**Mike O'Neal, Ph.D.**

*Independent scholar and writer*

Moscow, Idaho

**Belinda M. Rowland, Ph.D.**

*Science and medical writer*

Voorheesville, New York

**Judyth Sassoon, Ph.D., ARCS**

*Science writer with research experience in NMR and X-ray crystallography techniques*

Department of Biology & Biochemistry  
University of Bath, United Kingdom

**Morgan Simpson**

*Aerospace Engineer*

National Aeronautical and Space Administration (NASA)

Kennedy Space Center, Cape Canaveral, Florida

**Constance K. Stein, Ph.D.**

*Writer on medical and bioscience issues related to modern genetics*

Director of Cytogenetics, Assistant Director of Molecular Diagnostics

SUNY Upstate Medical University, Syracuse, New York

**Tabitha Sparks, Ph.D.**

*Marion L. Brittain fellow, Georgia Institute of Technology and Fellow, Center for Humanistic Inquiry, Emory University*

Atlanta, Georgia

**David Tulloch**

*Science and technology writer*

Wellington, New Zealand

**Michael T. Van Dyke, Ph.D.**

*Served as visiting assistant professor, Department of American Thought & Language*

Michigan State University, East Lansing, Michigan

**Stephanie Watson**

*Science writer specializing in the social impacts of science and technology*

Smyrna, Georgia

**Simon Wendt, Ph.D.**

*Ph.D. candidate in Modern History and History instructor*

John F. Kennedy Institute for North American Studies, Free University of Berlin, Germany

# ||| List of Entries |||

## | A |

Abu Nidal Organization (ANO)  
Abu Sayyaf Group (ASG)  
Abwehr  
ADFGX Cipher  
Aflatoxin  
Africa, Modern U.S. Security Policy and Interventions  
Agent Orange  
Air and Water Purification, Security Issues  
Air Force Intelligence, United States  
Air Force Office of Special Investigations, United States  
Air Marshals, United States  
Air Plume and Chemical Analysis  
Aircraft Carrier  
Airline Security  
Al-Aqsa Martyrs Brigade  
Alex Boncayao Brigade (ABB)  
Al-Gama'a al-Islamiyya (Islamic Group, IG)  
Al-Ittihad al-Islami (AIAI)  
Al-Jama'a al-Islamiyyah al-Muqatilah bi-Libya  
Al-Jihad  
Allied Democratic Forces (ADF)  
Al-Qaeda (also known as Al-Qaida)  
Americas, Modern U.S. Security Policy and Interventions  
Ames (Aldrich H.) Espionage Case  
Anthrax  
Anthrax, Terrorist Use as a Biological Weapon  
Anthrax Vaccine  
Anthrax Weaponization  
Antiballistic Missile Treaty  
Antibiotics  
Anti-Imperialist Territorial Nuclei (NTA)  
APIS (Advance Passenger Information System)  
Archeology and Artifacts, Protection of during War  
Architecture and Structural Security  
Area 51 (Groom Lake, Nevada)  
Argentina, Intelligence and Security  
Argonne National Laboratory  
Armed Islamic Group (GIA)  
Arms Control, United States Bureau

Army for the Liberation of Rwanda (ALIR)  
Army Security Agency  
'Asbat al-Ansar  
Asilomar Conference  
Assassination  
Assassination Weapons, Mechanical  
Asymmetric Warfare  
ATF (United States Bureau of Alcohol, Tobacco, and Firearms)  
Atmospheric Release Advisory Capability (ARAC)  
Audio Amplifiers  
Aum Supreme Truth (Aum)  
Australia, Intelligence and Security  
Austria, Intelligence and Security  
Aviation Intelligence, History  
Aviation Security Screeners, United States

## | B |

B-2 Bomber  
B-52  
Bacterial Biology  
Ballistic Fingerprints  
Ballistic Missile Defense Organization, United States  
Ballistic Missiles  
Balloon Reconnaissance, History  
Basque Fatherland and Liberty (ETA)  
Bathymetric Maps  
Bay of Pigs  
Belgium, Intelligence and Security Agencies  
Belly Buster Hand Drill  
Berlin Airlift  
Berlin Tunnel  
Berlin Wall  
Biochemical Assassination Weapons  
Biocontainment Laboratories  
Biodetectors  
Bio-Engineered Tissue Constructs  
Bio-Flips  
Biological and Biomimetic Systems  
Biological and Toxin Weapons Convention  
Biological Input/Output Systems (BIOS)



- Biological Warfare  
 Biological Warfare, Advanced Diagnostics  
 Biological Weapons, Genetic Identification  
 Bio-Magnetics  
 Biomedical Technologies  
 Biometrics  
 Bio-Optic Synthetic Systems (BOSS)  
 Biosensor Technologies  
 BioShield Project  
 Bioterrorism  
 Bioterrorism, Protective Measures  
 Black Chamber  
 Black Ops  
 Black Tom Explosion  
 Bletchley Park  
 Bolivia, Intelligence and Security  
 Bomb Damage, Forensic Assessment  
 Bomb Detection Devices  
 Bombe  
 Bosnia and Herzegovina, Intelligence and Security  
 Botulinum Toxin  
 Brain-Machine Interfaces  
 Brain Wave Scanners  
 Brazil, Intelligence and Security  
 British Terrorism Act  
 Brookhaven National Laboratory  
 Bubonic Plague  
 Bugs (Microphones) and Bug Detectors  
 Bush Administration (1989–1993), United States  
     National Security Policy  
 Bush Administration (2001–), United States  
     National Security Policy
- C**
- Cambodian Freedom Fighters (CFF)  
 Cambridge University Spy Ring  
 Cameras  
 Cameras, Miniature  
 Canada, Counter-Terrorism Policy  
 Canada, Intelligence and Security  
 Canine Substance Detection  
 Carter Administration (1977–1981), United States  
     National Security Policy  
 CDC (United States Centers for Disease Control  
     and Prevention)  
 CERN  
 Chechen-Russian Conflict  
 Chemical and Biological Defense Information  
     Analysis Center (CBIAC)  
 Chemical and Biological Detection Technologies  
 Chemical Biological Incident Response Force,  
     United States  
 Chemical Safety and Hazard Investigation Board  
     (USCSB), United States  
 Chemical Safety: Emergency Responses  
 Chemical Warfare  
 Chemistry: Applications in Espionage, Intelligence,  
     and Security Issues  
 Chernobyl Nuclear Power Plant Accident, Detection  
     and Monitoring  
 Chile, Intelligence and Security  
 China, Intelligence and Security
- Chinese Espionage against the United States  
 Church Committee  
 CIA (United States Central Intelligence Agency)  
 CIA (CSI), Center for the Study of Intelligence  
 CIA Directorate of Science and Technology (DS&T)  
 CIA, Foreign Broadcast Information Service  
 CIA, Formation and History  
 CIA, Legal Restriction  
 Cipher Disk  
 Cipher Key  
 Cipher Machines  
 Cipher Pad  
 Civil Aviation Security, United States  
 Civil War, Espionage and Intelligence  
 Classified Information  
 Clinton Administration (1993–2001), United States  
     National Security Policy  
 Clipper Chip  
 Closed-Circuit Television (CCTV)  
 Coast Guard (USCG), United States  
 Coast Guard National Response Center  
 Code Name  
 Code Word  
 Codes and Ciphers  
 Codes, Fast and Scalable Scientific Computation  
 COINTELPRO  
 Cold War (1945–1950), The Start of the Atomic Age  
 Cold War (1950–1972)  
 Cold War (1972–1989): The Collapse of the Soviet  
     Union  
 Colombia, Intelligence and Security  
 Colossus I  
 COMINT (Communications Intelligence)  
 Commerce Department Intelligence and Security  
     Responsibilities, United States  
 Commission on Civil Rights, United States  
 Communicable Diseases, Isolation, and Quarantine  
 Communications System, United States National  
 Comprehensive Test Ban Treaty (CTBT)  
 Computer and Electronic Data Destruction  
 Computer Fraud and Abuse Act of 1986  
 Computer Hackers  
 Computer Hardware Security  
 Computer Keystroke Recorder  
 Computer Modeling  
 Computer Security Act (1987)  
 Computer Software Security  
 Computer Virus  
 Concealment Devices  
 Consumer Product Safety Commission (CPSC),  
     United States  
 Continuity Irish Republican Army (CIRA)  
 Continuity of Government, United States  
 Continuous Assisted Performance (CAP)  
 Coordinator for Counterterrorism, United States  
     Office  
 Copyright Security  
 Counterfeit Currency, Technology and the  
     Manufacture  
 Counter-Intelligence  
 Counter-Terrorism Rewards Program  
 Covert Operations  
 Crib  
 Crime Prevention, Intelligence Agencies

Critical Infrastructure  
 Critical Infrastructure Assurance Office (CIAO),  
 United States  
 Croatia, Intelligence and Security  
 Cruise Missile  
 Cryptology and Number Theory  
 Cryptology, History  
 Cryptonym  
 Cuba, Intelligence and Security  
 Cuban Missile Crisis  
 Customs Service, United States  
 Cyanide  
 Cyber Security  
 Cyber Security Warning Network  
 Czech Republic, Intelligence and Security

## I D I

D Notice  
 DARPA (Defense Advanced Research Projects  
 Agency)  
 Data Mining  
 DCI (Director of the Central Intelligence Agency)  
 DEA (Drug Enforcement Administration)  
 Dead Drop Spike  
 Dead-Letter Box  
 Decontamination Methods  
 Decryption  
 Defense Information Systems Agency, United  
 States  
 Defense Nuclear Facilities Safety Board, United  
 States  
 Defense Security Service, United States  
 Delta Force  
 Department of State Bureau of Intelligence and  
 Research, United States  
 Department of State, United States  
 DIA (Defense Intelligence Agency)  
 Dial Tone Decoder  
 Diplomatic Security (DS), United States Bureau  
 Dirty Tricks  
 Disinformation  
 DNA  
 DNA Fingerprinting  
 DNA Recognition Instruments  
 DNA Sequences, Unique  
 Document Destruction  
 Document Forgery  
 DOD (United States Department of Defense)  
 DOE (United States Department of Energy)  
 Domestic Emergency Support Team, United States  
 Domestic Intelligence  
 Domestic Preparedness Office (NDPO), United  
 States National  
 Doo Transmitter  
 Dosimetry  
 Double Agents  
 Drop  
 Drug Control Policy, United States Office of  
 National  
 Drug Intelligence Estimates  
 Dual Use Technology

## I E I

E-2C  
 Ebola Virus  
 E-Bomb  
 Echelon  
 Economic Espionage  
 Economic Intelligence  
 Egypt, Intelligence and Security  
 Eichmann, Adolf: Israeli Capture  
 Eisenhower Administration (1953–1961), United  
 States National Security Policy  
 El Salvador, Intelligence and Security  
 Electromagnetic Pulse  
 Electromagnetic Spectrum  
 Electromagnetic Weapons, Biochemical Effects  
 Electronic Communication Intercepts, Legal Issues  
 Electronic Countermeasures  
 Electronic Warfare  
 Electro-Optical Intelligence  
 Electrophoresis  
 EM Wave Scanners  
 Emergency Response Teams  
 Encryption of Data  
 Enduring Freedom, Operation  
 Energy Directed Weapons  
 Energy Regulatory Commission, United States  
 Federal  
 Energy Technologies  
 Engraving and Printing, United States Bureau  
 Engulf, Operation  
 Enigma  
 Entry-Exit Registration System, United States  
 National Security  
 Environmental Issues Impact on Security  
 Environmental Measurements Laboratory  
 EPA (Environmental Protection Agency)  
 Epidemiology  
 Espionage  
 Espionage Act of 1917  
 Espionage and Intelligence, Early Historical  
 Foundations  
 Estonia, Intelligence and Security  
 European Union  
 Executive Orders and Presidential Directives  
 Explosive Coal

## I F I

F-117A Stealth Fighter  
 FAA (United States Federal Aviation  
 Administration)  
 Facility Security  
 FBI (United States Federal Bureau of Investigation)  
 FCC (United States Federal Communications  
 Commission)  
 FDA (United States Food and Drug Administration)  
 Federal Protective Service, United States  
 Federal Reserve System, United States  
 FEMA (United States Federal Emergency  
 Management Agency)  
 FEST (United States Foreign Emergency Support  
 Team)

Fingerprint Analysis  
 Finland, Intelligence and Security  
 First of October Anti-fascist Resistance Group (GRAPO)  
 FISH (German *Geheimschreiber* Cipher Machine)  
 Fission  
 Flame Analysis  
 Flight Data Recorders  
 FM Transmitters  
 FOIA (Freedom of Information Act)  
 Food Supply, Counter-Terrorism  
 Ford Administration (1974–1977), United States National Security Policy  
 Foreign Assets Control (OFAC), United States Office  
 Foreign Intelligence Surveillance Act  
 Foreign Intelligence Surveillance Court of Review  
 Forensic Geology in Military or Intelligence Operations  
 Forensic Science  
 Forensic Voice and Tape Analysis  
 France, Counter-Terrorism Policy  
 France, Intelligence and Security  
 French Underground during World War II, Communication and Codes  
 Fusion

## | G |

G–2  
 GAO (General Accounting Office, United States)  
 Gas Chromatograph-Mass Spectrometer  
 General Services Administration, United States  
 Genetic Code  
 Genetic Information: Ethics, Privacy and Security Issues  
 Genetic Technology  
 Genomics  
 Geologic and Topographical Influences on Military and Intelligence Operations  
 Geospatial Imagery  
 Germany, Counter-Terrorism Policy  
 Germany, Intelligence and Security  
 Gestapo  
 GIS  
 Global Communications, United States Office  
*Glomar Explorer*  
 Government Ethics (USOGE), United States Office  
 GPS  
 Great Game  
 Greece, Intelligence and Security  
 GSM Encryption  
 Guatemala, Intelligence and Security  
 Guerilla Warfare

## | H |

HAMAS (Islamic Resistance Movement)  
 Hanssen (Robert) Espionage Case  
 Harakat ul-Jihad-I-Islami (HUJI) (Movement of Islamic Holy War)

Harakat ul-Jihad-I-Islami/Bangladesh (HUJI-B) (Movement of Islamic Holy War)  
 Harakat ul-Mujahidin (HUM) (Movement of Holy Warriors)  
 Hardening  
 Health and Human Services Department, United States  
 Heavy Water Technology  
 Hemorrhagic Fevers and Diseases  
 Hizballah (Party of God)  
 Homeland Security, United States Department of  
 HUMINT (Human Intelligence)  
 Hungary, Intelligence and Security  
 Hypersonic Aircraft

## | I |

IBIS (Interagency Border Inspection System)  
 IDENT (Automated Biometric Identification System)  
 Identity Theft  
 IFF (Identification Friend or Foe)  
 IMF (International Monetary Fund)  
 IMINT (Imagery Intelligence)  
 India, Intelligence and Security  
 Indonesia, Intelligence and Security  
 Infectious Disease, Threats to Security  
 Information Security  
 Information Security (OIS), United States Office of Information Warfare  
 Infrared Detection Devices  
 Infrastructure Protection Center (NIPC), United States National  
 INS (United States Immigration and Naturalization Service)  
 INSCOM (United States Army Intelligence and Security Command)  
 INSPASS (Immigration and Naturalization Service Passenger Accelerated Service System)  
 Inspector General (OIG), Office of the Intelligence  
 Intelligence Agent  
 Intelligence and Counterespionage Careers  
 Intelligence and Democracy: Issues and Conflicts  
 Intelligence and International Law  
 Intelligence and Law Enforcement Agencies  
 Intelligence & Research (INR), United States Bureau of  
 Intelligence Authorization Acts, United States Congress  
 Intelligence Community  
 Intelligence Literature  
 Intelligence Officer  
 Intelligence Policy and Review (OIPR), United States Office of  
 Intelligence Support, United States Office of Intelligence, United States Congressional Oversight of  
 Interagency Security Committee, United States  
 Internal Revenue Service, United States  
 International Atomic Energy Agency (IAEA)  
 International Narcotics and Law Enforcement Affairs (INL), United States Bureau of

Internet  
 Internet: Dynamic and Static Addresses  
 Internet Spam and Fraud  
 Internet Spider  
 Internet Surveillance  
 Internet Tracking and Tracing  
 INTERPOL (International Criminal Police Organization)  
 Interpol, United States National Central Bureau  
 Interrogation  
 Interrogation: Torture Techniques and Technologies  
 Iran-Contra Affair  
 Iran, Intelligence and Security  
 Iranian Hostage Crisis  
 Iranian Nuclear Programs  
 Iraq, Intelligence and Security Agencies in  
 Iraq War: Prelude to War (The International Debate Over the Use and Effectiveness of Weapons Inspections)  
 Iraq War (Immediate Aftermath)  
 Iraqi Freedom, Operation (2003 War Against Iraq)  
 Ireland, Intelligence and Security  
 Irish Republican Army (IRA)  
 Islamic Army of Aden (IAA)  
 Islamic Movement of Uzbekistan (IMU)  
 Isotopic Analysis  
 Israel, Counter-Terrorism Policy  
 Israel, Intelligence and Security  
 Italy, Intelligence and Security

## | J |

Jaish-e-Mohammed (JEM) (Army of Mohammed)  
 Japan, Intelligence and Security  
 Japanese Red Army (JRA)  
 JDAM (Joint Direct Attack Munition)  
 Jemaah Islamiya (JI)  
 Johnson Administration (1963–1969), United States National Security Policy  
 Joint Chiefs of Staff, United States  
 Jordan, Intelligence and Security  
 J-STARS  
 Justice Department, United States

## | K |

Kahane Chai (Kach)  
 Kennedy Administration (1961–1963), United States National Security Policy  
 Kenya, Bombing of United States Embassy  
 KGB (*Komitet Gosudarstvennoi Bezopasnosti*, USSR Committee of State Security)  
 Khobar Towers Bombing Incident  
 Knives  
 Korean War  
 Kosovo, NATO Intervention  
 Kumpulan Mujahidin Malaysia (KMM)  
 Kurdistan Workers' Party (PKK)  
 Kuwait Oil Fires, Persian Gulf War

## | L |

Language Training and Skills  
 Laser  
 Laser Listening Devices  
 Lashkar-e-Tayyiba (LT) (Army of the Righteous)  
 Law Enforcement, Responses to Terrorism  
 Law Enforcement Training Center (FLETC), United States Federal  
 Lawrence Berkeley National Laboratory (LBL)  
 Lawrence Livermore National Laboratory (LLNL)  
 League of Nations  
 Lebanon, Bombing of U.S. Embassy and Marine Barracks  
 Less-Lethal Weapons Technology  
 L-Gel Decontamination Reagent  
 Liberation Tigers of Tamil Eelam (LTTE)  
 Libraries and Information Science (NCLIS), United States National Commission on  
 Libya, Intelligence and Security  
 Libya, U.S. Attack (1986)  
 LIDAR (Light Detection and Ranging)  
 Lock-Picking  
 Locks and Keys  
 Looking Glass  
 Lord Haw-Haw  
 Lord's Resistance Army (LRA)  
 Los Alamos National Laboratory  
 Loyalist Volunteer Force (LVF)

## | M |

Mail Sanitization  
 Malicious Data  
 Manhattan Project  
 Mapping Technology  
 Marine Mammal Program  
 McCarthyism  
 Measurement and Signatures Intelligence (MASINT)  
 Metal Detectors  
 Meteorology and Weather Alteration  
 Mexico, Intelligence and Security  
 MI5 (British Security Service)  
 MI6 (British Secret Intelligence Service)  
 Microbiology: Applications to Espionage, Intelligence, and Security  
 Microchip  
 Microfilms  
 Microphones  
 Microscopes  
 Microwave Weaponry, High Power (HPM)  
 Middle East, Modern U.S. Security Policy and Interventions  
 Military Police, United States  
 MOAB (Massive Ordnance Air Burst Bomb)  
 Molecular Biology: Applications to Espionage, Intelligence, and Security  
 Moles  
 Monroe Doctrine  
 Morocco, Intelligence and Security  
 Mossad  
 Motion Sensors

Mount Weather  
 Movies, Espionage and Intelligence Portrayals  
 Mujahedin-e Khalq Organization (MEK or MKO)  
 Mustard Gas

## I N I

NAIS (National Automated Immigration Lookout System)  
 Nanotechnology  
 Napoleonic Wars, Espionage during  
 NASA (National Air and Space Administration)  
 National Archives and Records Administration (NARA), United States  
 National Command Authority  
 National Drug Threat Assessment  
 National Information Infrastructure Protection Act, United States  
 National Intelligence Estimate  
 National Interagency Civil-Military Institute (NICI), United States  
 National Liberation Army (ELN)—Colombia  
 National Military Joint Intelligence Center  
 National Preparedness Strategy, United States  
 National Response Team, United States  
 National Security Act (1947)  
 National Security Advisor, United States  
 National Security Strategy, United States  
 National Security Telecommunications Advisory Committee  
 National Telecommunications Information Administration, and Security for the Radio Frequency Spectrum, United States  
 NATO (North Atlantic Treaty Organization)  
 Natural Resources and National Security  
 Navy Criminal Investigative Service (NCIS)  
 NCIX (National Counterintelligence Executive), United States Office of the  
 NDIC (Department of Justice National Drug Intelligence Center)  
 Near Space Environment  
 Nerve Gas  
 Netherlands, Intelligence and Security  
 New People's Army (NPA)  
 New Zealand, Intelligence and Security  
 NFIB (United States National Foreign Intelligence Board)  
 NIC (National Intelligence Council)  
 Nicaragua, Intelligence and Security  
 Nigeria, Intelligence and Security  
 Night Vision Scopes  
 NIH (National Institutes of Health)  
 NIJ (National Institute of Justice)  
 NIMA (National Imagery and Mapping Agency)  
 NIMH (National Institute of Mental Health)  
 NIST (National Institute of Standards and Technology), United States  
 NIST Computer Security Division, United States  
 Nixon Administration (1969–1974), United States  
 National Security Policy  
 NMIC (National Maritime Intelligence Center)  
 NNSA (United States National Nuclear Security Administration)

NOAA (National Oceanic & Atmospheric Administration)  
 Noise Generators  
 Nongovernmental Global Intelligence and Security  
 Non-Proliferation and National Security, United States  
 NORAD  
 North Korea, Intelligence and Security  
 North Korean Nuclear Weapons Programs  
 Norway, Intelligence and Security  
 NRO (National Reconnaissance Office)  
 NSA (United States National Security Agency)  
 NSC (National Security Council)  
 NSC (National Security Council), History  
 NSF (National Science Foundation)  
 NTSB (National Transportation Safety Board)  
 Nuclear Detection Devices  
 Nuclear Emergency Support Team, United States  
 Nuclear Power Plants, Security  
 Nuclear Reactors  
 Nuclear Regulatory Commission (NRC), United States  
 Nuclear Spectroscopy  
 Nuclear Weapons  
 Nuclear Winter  
 Nucleic Acid Analyzer (HANAA)

## I O I

Oak Ridge National Laboratory (ORNL)  
 Official Secrets Act, United Kingdom  
 OPEC (Organization of Petroleum Exporting Countries)  
 Operation Liberty Shield  
 Operation Magic  
 Operation Mongoose  
 Operation Shamrock  
 Orange Volunteers (OV)  
 OSS (United States Office of Strategic Services)

## I P I

P-3 Orion Anti-Submarine Maritime Reconnaissance Aircraft  
 Pacific Northwest National Laboratory  
 Pakistan, Intelligence and Security  
 Palestine Islamic Jihad (PIJ)  
 Palestine Liberation Front (PLF)  
 Palestinian Authority, Intelligence and Security  
 PanAm 103, (Trial of Libyan Intelligence Agents)  
 Panama Canal  
 Parabolic Microphones  
 Pathogen Genomic Sequencing  
 Pathogen Transmission  
 Pathogens  
 Patriot Act Terrorist Exclusion List  
 Patriot Act, United States  
 Patriot Missile System  
 Pearl Harbor, Japanese Attack on  
 People Against Gangsterism and Drugs (PAGAD)  
 Persian Gulf War  
 Peru, Intelligence and Security

Petroleum Reserves, Determination  
 PFIAB (President's Foreign Intelligence Advisory Board)  
 Phoenix Program  
 Photo Alteration  
 Photographic Interpretation Center (NPIC), United States National  
 Photographic Resolution  
 Photography, High-Altitude  
 Playfair Cipher  
 Plum Island Animal Disease Center  
 Poland, Intelligence and Security  
 Politics: The Briefings of United States Presidential Candidates  
 Pollard Espionage Case  
 Polygraphs  
 Polymerase Chain Reaction (PCR)  
 Popular Front for the Liberation of Palestine (PFLP)  
 Popular Front for the Liberation of Palestine-General Command (PFLP-GC)  
 Port Security  
 PORTPASS (Port Passenger Accelerated Service System)  
 Portugal, Intelligence and Security  
 Postal Security  
 Postal Service (USPS), United States  
 Potassium Iodide  
 President of the United States (Executive Command and Control of Intelligence Agencies)  
 Pretty Good Privacy (PGP)  
 Privacy: Legal and Ethical Issues  
 Profiling  
 Propaganda, Uses and Psychology  
 Pseudoscience Intelligence Studies  
 Psychotropic Drugs  
 Public Health Service (PHS), United States  
*Pueblo* Incident  
 Purple Machine

## I Q I

Quantum Physics: Applications to Espionage, Intelligence, and Security Issues

## I R I

RADAR  
 RADAR, Synthetic Aperture  
 Radiation, Biological Damage  
 Radio Direction Finding Equipment  
 Radio Frequency (RF) Weapons  
 Radioactive Waste Storage  
 Radiological Emergency Response Plan, United States Federal  
 Reagan Administration (1981–1989), United States National Security Policy  
 Real IRA (RIRA)  
 Reconnaissance  
 Red Code  
 Red Hand Defenders (RHD)  
 Red Orchestra  
 Remote Sensing

Retina and Iris Scans  
 Revolutionary Armed Forces of Colombia (FARC)  
 Revolutionary Nuclei  
 Revolutionary Organization 17 November (17 November)  
 Revolutionary People's Liberation Party/Front (DHKP/C)  
 Revolutionary Proletarian Initiative Nuclei (NIPR)  
 Revolutionary United Front (RUF)  
 Revolutionary War, Espionage and Intelligence  
 RF Detection  
 Ricin  
 Robotic Vehicles  
 Romania, Intelligence and Security  
 Room 40  
 Rosenberg (Ethel and Julius) Espionage Case  
 Russia, Intelligence and Security  
 Russian Nuclear Materials, Security Issues

## I S I

Sabotage  
 Salafist Group for Call and Combat (GSPC)  
 Salmonella and Salmonella Food Poisoning  
 Sandia National Laboratories  
 Sarin Gas  
 Satellite Technology Exports to the People's Republic of China (PRC)  
 Satellites, Non-Governmental High Resolution  
 Satellites, Spy  
 Saudi Arabia, Intelligence and Security  
 Scanning Technologies  
 SEAL Teams  
 Secret Service, United States  
 Secret Writing  
 Security Clearance Investigations  
 Security, Infrastructure Protection, and Counterterrorism, United States National Coordinator  
 Security Policy Board, United States  
 Seismograph  
 Seismology for Monitoring Explosions  
 Senate Select Committee on Intelligence, United States  
 Sendero Luminoso (Shining Path, or SL)  
 SENTRI (Secure Electronic Network for Travelers' Rapid Inspection)  
 September 11 Terrorist Attacks on the United States  
 Sequencing  
 Serbia, Intelligence and Security  
 Sex-for-Secrets Scandal  
 Ships Designed for Intelligence Collection  
 "Shoe Bomber"  
 Shoe Transmitter  
 Short-Wave Transmitters  
 SIGINT (Signals Intelligence)  
 Silencers  
 Skunk Works  
 Slovakia, Intelligence and Security  
 Slovenia, Intelligence and Security  
 Smallpox  
 Smallpox Vaccine

SOE (Special Operations Executive)  
 Soldier and Biological Chemical Command  
 (SBCCOM), United States Army  
 Solid-Phase Microextraction Techniques  
 Soman  
 SONAR  
 SOSUS (Sound Surveillance System)  
 South Africa, Intelligence and Security  
 South Korea, Intelligence and Security  
 Soviet Union (USSR), Intelligence and Security  
 Space Shuttle  
 Spain, Intelligence and Security  
 Spanish-American War  
 Special Collection Service, United States  
 Special Counsel and Security Related  
 “Whistleblower” Protection Issues, United States  
 Office  
 Special Operations Command, United States  
 Special Relationship: Technology Sharing between  
 the Intelligence Agencies of the United States  
 and United Kingdom  
 Spectroscopy  
 Spores  
 SR-71 Blackbird  
 START I Treaty  
 START II  
 STASI  
 Stealth Technology  
 Steganography  
 Strategic Defense Initiative and National Missile  
 Defense  
 Strategic Petroleum Reserve, United States  
 Sudan, Intelligence and Security  
 Suez Canal  
 Supercomputers  
 Surgeon General and Nuclear, Biological, and  
 Chemical Defense, United States Office  
 Sweden, Intelligence and Security  
 Switzerland, Intelligence and Security  
 Syria, Intelligence and Security

## III

Tabun  
 Taiwan, Intelligence and Security  
 Taser  
 Technical Intelligence  
 Technology Transfer Center (NTTC), Emergency  
 Response Technology Program  
 Telemetry  
 Telephone Caller Identification (Caller ID)  
 Telephone Recording Laws  
 Telephone Recording System  
 Telephone Scrambler  
 Telephone Tap Detector  
 Terror Alert System, United States  
 Terrorism, Domestic (United States)  
 Terrorism, Intelligence Based Threat and Risk  
 Assessments  
 Terrorism, Philosophical and Ideological Origins  
 Terrorism Risk Insurance  
 Terrorist and Para-State Organizations  
 Terrorist Organization List, United States

Terrorist Organizations, Freezing of Assets  
 Terrorist Threat Integration Center  
 Thin Layer Chromatography  
 TIA (Terrorism Information Awareness)  
 Tissue-Based Biosensors  
 Tokyo Rose  
 Toxicology  
 Toxins  
 Tradecraft  
 Transportation Department, United States  
 Treasury Department, United States  
 Truman Administration (1945–1953), United States  
 National Security Policy  
 Truth Serum  
 Tularemia  
 Tunisian Combatant Group (TCG)  
 Tupac Amaru Revolutionary Movement (MRTA)  
 Turkey, Intelligence and Security  
 Turkish Hizballah  
 Typex

## II

U-2 Incident  
 U-2 Spy Plane  
 Ukraine, Intelligence and Security  
 Ulster Defense Association/Ulster Freedom Fighters  
 (UDA/UVF)  
 Ultra, Operation  
 Underground Facilities, Geologic and Structural  
 Considerations in the Construction  
 Undersea Espionage: Nuclear vs. Fast Attack Subs  
 Unexploded Ordnance and Mines  
 United Kingdom, Counter-Terrorism Policy  
 United Kingdom, Intelligence and Security  
 United Nations Security Council  
 United Self-Defense Forces/Group of Colombia  
 (*AUC Autodefensas Unidas de Colombia*)  
 United States, Counter-Terrorism Policy  
 United States, Intelligence and Security  
 United States Intelligence, History  
 Unmanned Aerial Vehicles (UAVs)  
 Uranium  
 Uranium Depletion Weapons  
 USAMRICD (United States Army Medical Research  
 Institute of Chemical Defense)  
 USAMRIID (United States Army Medical Research  
 Institute of Infectious Diseases)  
 USS *Cole*  
 USS *Liberty*  
 USSTRATCOM (United States Strategic Command)

## III

Vaccination  
 Vaccines  
 Variola Virus  
 Venezuela, Intelligence and Security  
 Venona  
 Vietnam War  
 Viral Biology

Viral Exposure Therapy, Antiviral Drug  
Development  
Voice Alteration, Electronic  
Voice of America (VOA), United States  
Vozrozhdeniye Island, Soviet and Russian  
Biochemical Facility  
Vulnerability Assessments  
VX Agent

## W

Walker Family Spy Ring  
War of 1812  
Water Supply: Counter-Terrorism  
Watergate  
Weapon-Grade Plutonium and Uranium, Tracking  
Weapons of Mass Destruction

Weapons of Mass Destruction, Detection  
Windtalkers  
World Health Organization (WHO)  
World Trade Center, 1993 Terrorist Attack  
World Trade Center, 2001 Terrorist Attack  
World War I  
World War I: Loss of the German Codebook  
World War II  
World War II: Allied Invasion of Sicily and “The  
Man Who Never Was”  
World War II, The Surrender of the Italian Army  
World War II, United States Breaking of Japanese  
Naval Codes

## Z

Zoonoses



*This page intentionally left blank*



---

## RADAR

---

■ LARRY GILMAN

RADAR—an acronym for RAdio Detection And Ranging—is the use of electromagnetic waves at sub-optical frequencies (i.e., less than about  $10^{12}$  Hz) to sense objects at a distance. Hundreds of different RADAR systems have been designed for various purposes, military and other. RADAR systems are essential to the navigation and tracking of craft at sea and in the air, weather prediction, and scientific research of many kinds.

**Principles.** In basic RADAR, radio waves are transmitted from an antenna. These outgoing waves eventually bounce off some distant object and return an echo to the sender, where they are received, amplified, and processed electronically to yield an image showing the object's location. The waves sent out may be either short oscillatory bursts (pulses) or continuous sinusoidal waves. If a RADAR transmits pulses it is termed a pulse RADAR, whereas if it transmits a continuous sinusoidal wave it is termed a continuous-wave RADAR.

On closer examination, the RADAR process is seen to be more complex. For example, reflection of an echo by the object one wishes to sense is anything but straightforward. Upon leaving a transmitting antenna, a radio wave propagates in a widening beam at the speed of light ( $> 186,000$  miles per hour [ $3 \times 10^8$  m/sec]); if it encounters an obstacle (i.e., a medium whose characteristic impedance differs from that of air and vacuum [ $> 377 \Omega$ ]), it splits into two parts. One part passes into the obstacle and is (generally) absorbed, and the other is reflected. Where the reflected wave goes depends on the shape of the obstacle. Roundish or irregular obstacles tend to scatter energy through a wide angle, while flat or facet-like surfaces tend to send it off in a single direction, just as a flat mirror reflects light. If any part of the outgoing wave is reflected

at  $180^\circ$  (which is not guaranteed) it will return to the transmitter. This returned or backscattered signal is usually detected by the same antenna that sent the outgoing pulse; this antenna alternates rapidly between transmitting pulses and listening for echoes, thus building a real-time picture of the reflecting targets in range of its beam. The energy the echoes receive is a small fraction of that in the pulses transmitted, so the strength of the transmitted pulse and the sensitivity of the receiver determines a RADAR's range. By systematically sweeping the direction in which its antenna is pointed, a RADAR system can scan a much larger volume of space than its beam can interrogate at any one moment; this is why many RADAR antennas, on ships or atop air-traffic control towers, are seen to rotate while in operation.

Radio waves are not the only form of energy that can be used to derive echoes from distant targets. Sound waves may also be used. Indeed, because radio waves are rapidly absorbed in water, sonar (SOund Navigation and Ranging) is essential to underwater operations of all sorts, including sea-floor mapping and anti-submarine warfare.

**Applications.** Since World War II RADAR has been deployed in many forms and has found a wide application in scientific, commercial, and military operations. RADAR signals have been bounced off targets ranging in size from dust specks to other planets. RADAR is essential to rocketry and early-warning detection of missiles, air traffic control, navigation at sea, automatic control of weapons such as antiaircraft guns, aircraft detection and tracking, mapping of the ground from the air, weather prediction, intruder detection, and numerous other tasks. Few craft, military or civilian, put to sea or take to the air without carrying some form of RADAR.

In recent decades, development of the basic RADAR principle—send pulse, listen for echo—has proceeded along a number of interesting paths. By exploiting the Doppler effect, which causes frequency shifts in echoes reflected from moving objects, modern RADARs can tell not only where an object is but what direction it is moving

in and how quickly. The Doppler effect also allows for the precision mapping of landscapes from moving aircraft through the synthetic-aperture technique. Synthetic-aperture systems exploit the fact that stationary objects being swept by a RADAR beam projected from a moving source have, depending on their location, slightly different absolute velocities with respect to that source. By detecting these velocity differences using the Doppler effect, synthetic aperture type RADAR greatly permits the generation of high-resolution ground maps from small, airborne RADARs.

In many modern RADAR systems the need for a mechanically moving antenna has been obviated by phased arrays. A phased array consists of a large number of small, computer-controlled antennas termed elements. These elements, of which there are usually thousands, are crowded together to form a flat surface. In transmit mode, the elements are all instructed to emit a RADAR pulse at approximately the same time; the thousands of outbound waves produced by the elements merge into a single powerful wave as they spread outward. By timing, or *phasing*, the elements in the array so that, for example, elements along the left-hand edge of the array fire first while those farther to the right fire progressively later, the composite wave formed by the merging of the elements' lesser outputs can be steered in any desired direction within a wide cone (in this example, to the right). Beam steering can be accomplished by such a system millions of times more rapidly than would be possible with mechanical methods. Phased-array systems are used for a number of applications; including the 71.5-foot (21.8-m) tall AN/FPS-115 PAVE PAWS Early Warning RADAR Array Antennas, which provide early warning of ballistic-missile attack; shipboard systems such as the AN/SPY-1D, which is about 15 feet (3 m) across and is mounted flush with the upper hull of some warships; the Hughes AN/TPQ-37 Firefinder, a trailer-mounted system designed for tracking incoming artillery and missiles and calculating their point of origin; and many other real-world systems.

RADAR is a powerful weapon of war, but has its weaknesses. For example, numerous missiles have been developed to home in on the radio pulses emitted by RADARs, making it very dangerous to turn on a RADAR in a modern battlefield situation. Further, jamming and spoofing ("electronic warfare") have evolved rapidly alongside RADAR itself. For example, an aircraft that finds itself interrogated by a RADAR pulse can emit blasts of noise or false echoes, or request that a drone or other unit emit them, in order to confuse enemy RADAR. Finally, aircraft have been built that are "low observable," that is, which scatter very little energy back toward any RADAR that illuminates them. Low-observable or "stealth" aircraft are built of radio-absorbent materials and shaped to present little or no surface area perpendicular to RADAR pulses approaching from most angles (except directly above and directly below, the two least likely places for an enemy RADAR to be at any given moment). What RADAR they do reflect is deflected at low angles rather than returned to

the RADAR transmitter. The U.S. B-2 bomber and F-117A and F-22 fighters are working examples of low-observable aircraft.

#### ■ FURTHER READING:

##### BOOKS:

Edde, Byron. *RADAR: Principles, Technology, Applications*. Englewood Cliffs, NJ: PTR Hall, 1993.

Skolnik, Merrill I. *Introduction to RADAR Systems*. New York: McGraw Hills, 2001.

##### SEE ALSO

*Stealth Technology*  
*RADAR, Synthetic Aperture*

## RADAR Detection Avoidance.

SEE *Stealth Technology*.

---

## RADAR, Synthetic Aperture

---

Synthetic aperture RADAR (SAR) is used for high-resolution mapping of the ground from moving aircraft or spacecraft. A stationary RADAR system's angular resolution—that is, the clarity with which it can distinguish two small, side-by-side targets at a given distance—is determined by the physical width (aperture) of its antenna. By appropriate processing of the echoes received by a small, but moving antenna, an angular resolution equivalent to that of a much larger antenna can be synthesized—hence the term "synthetic aperture RADAR" for such a system.

SAR exploits the Doppler effect, a property of waves reflected (or emitted) by moving objects. If a wave is reflected or emitted by an object approaching a receiver, its frequency as perceived by the receiver is raised; if the object is receding, its frequency is perceived by the receiver as lowered. Most people have noticed the Doppler effect when a vehicle blowing its horn passes them at high speed; the sound of the horn is high-pitched when the vehicle is approaching, then drops when the vehicle passes by. Basic SAR works as follows: first, a narrow, fan-shaped radar beam is projected at right angles to the forward motion of an aircraft (or other platform). Distant objects cut across this side-looking beam as the aircraft moves in a straight line. As an object first enters the beam, its relative motion has a component that is toward the aircraft and which Doppler-shifts its RADAR reflection to higher frequencies. As the object passes through the centerline of the beam, it ceases to get closer to the aircraft. At this fraction of a second, its reflection ceases to be Doppler shifted. Next, as the object passes through the trailing half

of the beam, it begins to move away from the aircraft, which Doppler-shifts its reflection to lower frequencies. Thus, although reflections from all objects at a given distance from the RADAR return to its antenna at the same moment, reflections from objects ahead of the aircraft are Doppler shifted to higher frequencies, and those from objects trailing the aircraft are shifted to lower frequencies. This effect can be used to distinguish objects inside the beam, achieving an angular resolution that is higher than the beam's physical width.

SAR mapping was first demonstrated in 1953 and has since been widely used by the military (with various refinements) for airborne battlefield surveillance. SAR has also been used for satellite-based radar mapping of the Earth and Venus.

#### ■ FURTHER READING:

##### BOOKS:

- Edde, Byron. *RADAR: Principles, Technology, Applications*. Englewood Cliffs, NJ: PTR Prentice Hall, 1993.
- Fitch, J. Patrick. *Synthetic Aperture RADAR*. West Hanover, MA: Springer-Verlag, 2001.

##### SEE ALSO

RADAR

---

## Radiation, Biological Damage

---

- ABDEL HAKIM BEN NASR
- BRIAN HOYLE

The nuclear explosions at Hiroshima and Nagasaki, Japan on August 6 and 9, 1945, demonstrated the immense power of the nuclear bomb. The effects of the explosion were immediate. The radiation that was released by the explosions, however, caused the deaths of many people weeks, months, and even years later. It is this radiation-induced biological damage that can ultimately claim more lives than those lost in the blast of a nuclear weapon.

Radiation released in a nuclear explosion consists of particles that have a high energy. When these particles encounter biological material, in particular deoxyribonucleic acid (DNA), they can break the DNA strands. The breakage can be so severe that a cell's repair machinery cannot compensate. Because DNA is the blueprint for the structure and all the activities that occur in cells, the radiation-induced damage to DNA is lethal to the affected cells.

Radiation exposure that does not kill cells outright can cause sublethal damage that scrambles the sequence of information contained in the DNA. As a result, when the DNA is used to make proteins, proteins that are altered

from the intended forms will be made. These represent mutations.

Mutations occur naturally at a very low rate. Using special agents called mutagens can increase the frequency of these mutations. Ionizing radiation was the first mutagen that efficiently and reproducibly induced mutations in a multicellular organism. Radiation is often classified as ionizing or non-ionizing depending on whether ions are emitted in the penetrated tissues or not. Examples of ionizing radiation include x rays, gamma rays, beta particle radiation, and alpha particle radiation (also known as alpha rays). The ultraviolet radiation that is a component of sunlight is an example of a nonionizing radiation.

Different types of radiation have different energies, and so have different effects. With alpha radiation, ionizations produce an intense but more superficial and localized deposition of energy. The energy of x rays and gamma radiation traverses deeper into tissues. This penetration leads to a more even distribution of energy as opposed to the more concentrated or localized alpha rays.

The different behaviors of different types of radiation can be used to some extent to tailor the radiation to selected cellular components. Experiments conducted on animals have shown that repeated exposure to radiation produces a higher frequency of mutations than a single exposure to a higher level of radiation. In other words, exposure to a low level of radiation can be damaging over time.

The relative efficiencies of the different types of radiation in producing mutations can be compared, and is known as the mutagenic effect. Investigation of radiation's mutagenic effects on different tissues, cells, and subcellular compartments is becoming possible by the availability of techniques and tools that allow the precise delivery of small doses of radiation and that provide better monitoring of effects.

Cells that are irradiated release a form of oxygen that is unstable, and which reacts with cellular components in a way that is damaging. DNA can be damaged, as can components called bases, which are assembled to form DNA strands. As well, the reactive oxygen can damage enzymes that function to repair damaged DNA. There is evidence that radiation damage in one cell can be passed on to neighbouring cells. Even the neighbouring cells may be damaged genetically. Thus, radiation damage, especially due to low levels of radiation, may be more extensive than previously assumed.

This increased risk of radiation damage is of concern, as terrorist organizations such as al Qaeda have made efforts to develop and deploy "dirty bombs"—conventional explosives that release a payload of radioactive material. In 2002, an American citizen was arrested for his alleged involvement with al Qaeda to detonate a dirty bomb inside the United States. The spray of radiation in a mid-level dirty bomb could produce a relatively low level of radiation over a fairly localized area. In a densely populated city, thousands of people could be exposed to

harmful levels of radiation from an explosion from a dirty bomb.

#### ■ FURTHER READING:

##### BOOKS:

Cheung, Kin P. *Plasma Charging Damage*. Berlin: Springer Verlag, 2000.

Mangano, Joseph, J. *Low level radiation and Immune System Damage: An Atomic Era Legacy*. Boca Raton: Lewis Publishers, 1998.

##### PERIODICALS:

Azzam, E. I., S. M. de Toledo, and J. B. Little. "Direct evidence for the participation of gap junction-mediated intercellular communication in the transmission of damage signals from alpha-particle irradiated to nonirradiated cells." *Proceedings of the National Academy of Sciences* no. 98 (2001): 473–478.

##### SEE ALSO

*Nuclear Detection Devices*  
*Weapons of Mass Destruction, Detection*

---

## Radio Direction Finding Equipment

---

One of the earliest military applications for radio was in direction-finding (DF), which makes it possible to locate the positions of enemy aircraft and ships using four major components: an antenna, a receiver, a processor or processors, and a control and output system. Examples of radio DF equipment in use at the beginning of the twenty-first century include the OUTBOARD (Organizational Unit Tactical Baseline Operational Area Radio Detection) system of the U.S. Navy. Direction finding often uses triangulation, which is based on laws of plane trigonometry.

**Direction finding and triangulation.** A direction finder can be any electronic device used to locate a source of electronic emissions such as a ship or aircraft. In everyday usage by military, security, and intelligence services, direction finding is virtually synonymous with radio DF. Direction finding usually involves a radio receiver linked to a revolving antenna, which scans for the strongest possible signal in the area.

Assuming two stationary transmitters can be located, direction finding can be used to locate one's position by means of triangulation. The latter is based on the trigonometric principle that, for any triangle, when one side and

two angles are known, the other angle and two sides can be calculated. To establish the measure for two angles of a triangle on Earth's surface, it is necessary to use a surveying device known as a theodolite, or some electronic equivalent. The measured and known side of the triangle is known as the baseline.

**Components of a DF system.** The simplest DF system must contain an antenna, receiver, at least one processor, and control/output systems. The antenna must be versatile, so as to address a variety of requirements, some of which seem almost at cross-purposes to one another. It must be omnidirectional, or capable of receiving input from 360 degrees, yet capable of pinpointing the locations of specific signals from the range of radio noise it receives. Additionally, it must make possible the reception of signals over the widest possible area, yet receive these on an ultra-accurate pencil beam. Given these various requirements, modern DF systems often use not one antenna but an array, or they may make use of a phased-array antenna, which can quickly change its pattern of radiation using electronic means.

Receivers may be either single-channel, dual-channel, or N-channel. In a single-channel receiver, a switch sequentially selects one antenna from an array, while in the dual-channel model, switching may be used to select pairs from three or more antennas. N-channel receivers are capable of operating across multiple antennas without the requirement of switching.

Once the signal is received, it is necessary to calculate the location of the emitter by comparing signal properties such as amplitude. For this operation, a processor is used. With multiple or phased-array antennas, the operator may need not a single processor, but an array of distributed digital signal processors. With twenty-first century technology, it is possible for machines to perform a variety of complex calculations in real time or near-real time. Lastly, there is the control/output system, which includes a variety of subcomponents such as functions for the input and preparation of data, as well as various other operations requiring a workable interface between operator and equipment.

**Radio DF in history.** The use of radio direction finding dates back to World War I, when both the Allies and the forces of the Central Powers used it to locate enemy positions on the ground. The essential principles of direction-finding were established at that time, well before radio entered commercial use in the early 1920s.

During the interwar period, the British Royal Navy used radio DF extensively with the aid of listening stations. The latter had been established in the wake of escalating international conflicts, including the Italian invasion of Ethiopia (which potentially threatened British-controlled lands in east Africa) and the Spanish Civil War,

during which Italian submarines threatened British vessels transporting supplies to Republican forces.

By the late 1930s, the British had begun using high-frequency direction finding (HF/DF or "Huff Duff") equipment on their warships. This technology had benefited from improvements by Canadian engineers, who created a means of automatically recording the directional bearings of transmissions by radio. During the Second World War, the Royal Navy successfully used HF/DF to locate German submarines in the north Atlantic.

Across the ocean, the U.S. Navy received help from French scientists who had escaped the Nazi and Vichy regimes, and who assisted Navy technicians in developing a means of visual imaging to record the bearings of a vessel emitting transmissions. This equipment, tested in 1940 and operational by the latter part of 1942, also made it possible to maintain a track on an enemy U-boat even after the latter had stopped transmitting.

**DF in the Cold War and modern era.** The Germans themselves made advances in antenna technology, but because of their failure to accurately assess Allied DF capabilities, the principal beneficiaries of these developments would later be their wartime adversaries. During the 1950s and 1960s, the U.S. military adapted German Wullenweber antenna systems for use in Vietnam and other theatres of the Cold War. The United States also made use of the Wullenwebers (sometimes referred to as circularly disposed dipole antenna arrays or CDDAs) for land-based electronic eavesdropping, taking advantage of their wide operational range of 3,200 miles (5,150 km). Today, abandoned Wullenwebers—nicknamed "rings of poles," "dinosaur cages," or "elephant cages"—dot the globe, an almost poignant visual symbol of the long-vacated superpower conflict.

At the turn of the twenty-first century, radio DF equipment was a standard feature of U.S. Navy vessels. By 2000, the OUTBOARD system had been in use on naval vessels for many years, and was slated for an upgrade through the Cooperative OUTBOARD Logistics Update (COBLU) program. OUTBOARD made use of high-frequency deck-edge antennas and VHF (very high frequency) mast antennas, as well as a receiver that automatically searched for, received, collected, and analyzed signals. Thus, it combined the receiving and processing functions in a single piece of equipment. Its control/output system is capable of collecting processed cryptologic transmissions and transmitting intelligence to other members of the battle group via data links.

#### ■ FURTHER READING:

##### PERIODICALS:

Cochran, William W. "Direction Finding at Ultra High Frequency (UHF): Improved Accuracy." *Wildlife Society Bulletin* 29, no. 2 (summer 2001): 594.

##### ELECTRONIC:

Herskovitz, Don. "A Sampling of Direction-Finding Systems." *Journal of Electronic Defense* 23, no. 8 (August 2000): 57–65.

Rivers, Brendan. "U.S. Navy Orders OUTBOARD Update." *Journal of Electronic Defense* 23, no. 8 (August 2000): 31.

Robinson, Clarence O., Jr. "Position-Fixing Methods Use Broadband Direction Finders." *Signal* 53, no. 2 (October 1998): 71–74.

##### SEE ALSO

*Electronic Countermeasures*  
*Electronic Warfare*  
*FM Transmitters*  
*GPS*  
*SIGINT (Signals Intelligence)*

## Radio Frequency (RF) Weapons

RF, or radio frequency weapons, also known as directed-energy weapons, use electromagnetic energy on specific frequencies to disable electronic systems. The principle is similar to that of high-power microwave (HPM) weapons, only HPM systems tend to be much more sophisticated, and are thus, more likely to be in the control of superpowers or near-superpowers. RF weapons, by contrast, are simple and low-voltage enough that they could be deployed by smaller, less technologically enhanced forces.

The range of frequencies for waves in the electromagnetic spectrum is from approximately  $10^2$  Hz to more than  $10^{25}$  Hz—in other words, from about 100 cycles per second to about 10 trillion trillion. From the lowest frequencies to about  $10^{10}$  Hertz is the range of long-wave radio, short-wave radio, and microwaves. These carry broadcast radio, television, mobile phone communications, radar, and even highly specific forms of transmission such as those of baby monitors or garage-door openers.

Because of regulation by the Federal Communications Commission (FCC), AM or amplitude modulation broadcasts take place across a frequency range from 535 kHz (kilohertz, or 1,000 Hertz) to 1.7 MHz (megahertz, or 1,000,000 Hertz). The FCC has assigned the range of 5.9 to 26.1 MHz to shortwave radio, and 26.96 to 27.41 MHz to citizens' band (CB) radio. Above these are microwave regions assigned to very high frequency (VHF) television stations 2 through 6, then FM (frequency modulation) radio, which occupies the range from 88 to 108 MHz. Higher still are VHF channels 7 to 13, ultra-high frequency (UHF) television broadcasts, and so on. At the highest

microwave ranges—around  $10^{10}$  Hz—are transmissions from spacecraft.

FCC regulation is necessary to maintain security, privacy, and safety on the airwaves. If a broadcaster or receiver strays outside of its assigned range, it can intercept private communications, or potentially disrupt highly sensitive transmissions. Among the most sensitive from a safety perspective, are the communications between an aircraft cockpit and the control tower, which could result in serious consequences if disrupted even for a few seconds.

High-power microwave weaponry is of such voltage and intensity that it can actually shut off the computer systems of an aircraft long enough that a pilot could conceivably be unable to right the craft, causing a crash. With an RF weapon, the intensity of the signal is smaller, but if properly directed, it could potentially disrupt aircraft communication systems long enough to bring down the craft. It could cause the computers to reset, or disrupt safety sensors, navigation systems, data recorders, or control systems. Enough errors in these sensitive flight components, particularly in the highly computerized aircraft of today, might be enough to force a plane out of the sky.

Concerns over RF interference dictate the prohibition against cell phone, radio, or even laptop computer operation aboard a plane from the time of preparation for takeoff until after it lands. Such relatively weak and innocuous systems could interfere with vital flight communications; one can easily imagine the harm that could be done by terrorists operating a directed and more powerful system with malicious intent. Adding to the dangers of RF weaponry is the fact that it could potentially be operated from the ground, allowing the terrorist to attack and seek cover in the process, and rendering the sacrifice of the terrorist's life unnecessary. Furthermore, RF weaponry, like most means of electromagnetic warfare, is "clean," meaning that, unlike ordinary ballistic weaponry, it is almost untraceable.

## ■ FURTHER READING:

### PERIODICALS:

Larson, Virgil. "The Next Wave: Using Radio Frequency as Weapon." *Omaha World-Herald*. (April 14, 2002): 1D.

"Moscow, Tehran to Discuss RF Weapons Supplies to Iran—VP." *Itar-Tass News Wire*. (February 28, 2001): 1.

"Russia Developing New Radio Frequency Weapons." *Electromagnetic News Report* 30, no. 2 (March/April 2002): 1.

### SEE ALSO

*E-Bomb*

*Electromagnetic Pulse*

*Electronic Countermeasures*

*Electronic Warfare*

*Microwave Weaponry, High Power (HPM)*

## Radioactive Waste Storage

■ ADRIENNE WILMOTH LERNER

The storage of radioactive waste generated by the use and production of radioactive materials within the United States remains a contentious national security issue. The security of these materials, many taking thousands of years to decay, requires not only security measures to prevent tampering or theft, but also important considerations of the physical environment of waste storage. Site selection must ultimately be based upon minimizing the potential for leakage and long-term environmental damage.

In the 1960s, nuclear power gained popularity as a means of producing electricity for civilian use. During the next two decades, several nuclear power plants were built, but there was little consensus about how to best dispose of radioactive waste. Waste from plants, as well as from military and defense operations, was usually stored on site or in nearby storage facilities. Low-level waste, such as that from hospitals, research labs, and power plants is generally placed into containment facilities on-site. However, the disposal of high-level waste, materials that are highly radioactive, remains more problematic. Spent nuclear fuels from power plants are sometimes shipped to containment facilities, and sometimes stored in specially constructed containment pools on-site. Radioactive waste is thus, stored in various locations, governed by federal regulations. Forty-three states in the United States, and several Canadian provinces, currently have nuclear waste storage facilities. In the late 1990s, the government proposed plans for a central storage facility for high-level waste at Yucca Mountain, Nevada. In May, 2002, the United States House of Representatives approved a measure that would establish the site at Yucca Mountain, and approval was pending as of June 2002. The proposed site has sparked ongoing controversy over the environmental impact of nuclear waste storage, much of which focuses on the unique geological and environmental conditions of the region.

When looking for a site for permanent storage of high level waste, engineers and geologists took several factors into consideration, including: water table, geological stability, rock composition, seismic (earthquake) activity, and proximity to population areas. Furthermore, the site must have a high probability of remaining undisturbed for tens of thousands of years, or as long as the materials in storage are radioactive. Yucca Mountain is located in a rural region, with sparse population. Las Vegas, 100 miles (160 km) from the site, is the nearest metropolitan area. Within a 100-mile radius of the proposed site, there are approximately 35,000 inhabitants. Thus, Yucca Mountain is relatively secluded.

Yucca Mountain itself has a desert climate, receiving less than six inches of rain per year. The lack of rain means that cave systems within the mountain are dry, and that

there is minute seepage from the surface of the mountain to the deep water table 2000 feet (670 meters) below ground. This ensures that waste stored in the mountain would have fewer chances of polluting ground water if specially engineered storage containers ever rupture. The deep location of the water table at the site also means that the cavity, or storage room, would lie equidistant from the surface of the mountain to ground water stores—about 1000 feet, or 304 meters. This isolates the waste, and removes the chance of accidental disturbance from future drilling or other means of exploration.

Some aspects of the geological composition of the mountain itself further makes Yucca Mountain a candidate for a nuclear waste repository. Dense volcanic rock, as well as thick and nearly impenetrable bedrock mean Yucca Mountain's interior is relatively stable, not very porous, and resistant to water and heat. Under the most extreme conditions, this deep and solid rock could help contain minor seepage, as well as insulate the repository—possibly making it as safe as a band of untapped uranium ore.

Yucca Mountain's unique geology and environment is unequaled by that of any of the nation's other current nuclear waste repositories, many of which pose a greater potential threat to cities, drinking water, and their local environments. Centralization could potentially lead to tighter regulation of waste, better handling, and less environmental damage.

While Yucca Mountain does meet much of the criteria for a safe storage site, it is not a perfect location. The region around Yucca Mountain contains several faults and fractures (cracks in the Earth's crust where movement causes earthquakes), and is considered seismically active. Earthquakes could change the patterns of water flow inside the mountain, as well as endanger the integrity of the storage cavities within the mountain. Increased hydrothermal activity could promote seepage and water contamination.

Researchers also explored the possibility of the storage cavity filling with water, thus exposing the aquifer and groundwater to radioactive contaminants. Geologists studied core samples and cave linings to determine the extent to which minerals permeated the walls of the cavities. The scientists found that there were only scant traces of opal and calcite, telltale signs of flooding and water seepage, at the lower levels of the mountain. Thus, the cavities did not have a history of filling with water. A corresponding study of the geological history of the mountain further confirmed the relative stability of the site's water table, drainage, and seepage.

However, under Yucca Mountain is a deep aquifer. In the desert region, the aquifer provides drinking and irrigation water. As metropolitan centers, such as Las Vegas, continue to grow, the aquifer might play a significant role as a water resource for the region. The nuclear storage site would have to remain stable and well sealed for tens of thousands of years in order to insure the continued safety of the aquifer.

Part of the problem in designing high-level waste storage facilities is the time span for which these sites must remain secure and safe. Lab tests are inadequate to insure the stability of the mountain, the fortitude of containers and casks, and the security of the site from accidental intrusion for the tens of thousands of years necessary for radioactive waste to be rendered harmless. Project planners face not only design difficulties such as preventing accidents and mitigating environmental impact, but also how to document the site in ways that will ensure that people 10,000 years from now will recognize the hidden danger of the mountain storage facility. People today have only scant artifacts and generalized understanding of civilizations and people that lived ten thousand years ago.

Geologists and other scientists disagree on the possible effect that the waste could have on the behavior of the mountain itself. Some predict that heat generated by the waste could alter the mountain's geological and hydrological behavior, causing rocks to crack and water to seep into and out of the storage cavity in ways that we cannot predict. Some raise concerns over the unpredictable nature of seismic activity in the area. Other scientists assert that the stable pattern of geological processes at Yucca Mountain will remain unchanged, and that the site is predictably stable. Geologists have to account for not only the mountain's history, but also predict its future in order to insure the safety of the site for future generations.

While much of the scientific community's assessment of the safety of the Yucca Mountain project centers on geology, public concerns focus on technology. Though waste is currently stored in forty-three states, little of the nation's spent nuclear materials travel long distances. The creation of the Yucca Mountain site would require that waste be shipped by truck and rail to the central storage facility. Engineers and researchers have developed safe casks, or storage bins, which are impervious to accidents, water, and fire specifically for shipping high-level waste, but many people are discomfited simply by the perceived risk (the threat that people feel is associated with a given project, not the statistical risk) of shipping nuclear materials.

The controversy surrounding the proposed Yucca Mountain waste repository is both political and scientific. The perceived threat of nuclear materials heavily influences public opinion, and environmentalists are reticent to trade many smaller environmental problems for a large potential hazard. Some people cite the Yucca Mountain facility as a means of centralizing the problem of nuclear waste. Project proponents claim that the repository will lessen environmental risk and keep volatile, dangerous materials secure and controlled.

#### ■ FURTHER READING :

##### BOOKS:

Bechthold, W., et al. *Direct Disposal of Spent Nuclear Fuel (Radioactive Waste Management Series)*. N.p., Graham & Trotman, 1988.



Hafner, R. S., ed. "Transportation, Storage, and Disposal of Radioactive Materials: Presented at the 1999 *Asme Pressure Vessels and Piping Conference*." American Society of Mechanical Engineers, 1990.

SEE ALSO

*NNSA (United States National Nuclear Security Administration) Nuclear Power Plants, Security Nuclear Reactors*

## Radiological Emergency Response Plan, United States Federal

The Federal Radiological Emergency Response Plan (FRERP) is a blueprint for the response of the United States federal government to a radiological emergency—that is, a crisis involving the release of nuclear radiation. Drafted by a Federal Emergency Management Agency (FEMA) committee in 1985, FRERP is an agreement among 17 federal agencies, key among which are FEMA, the Nuclear Regulatory Commission (NRC), the Departments of Energy and Defense, and the Environmental Protection Agency (EPA).

### Roots of the FRERP

From the time of its founding in 1970, EPA had responsibility for dealing with radiological emergencies, though an orchestrated federal response to such situations still lay many years in the future. In 1975, the General Services Administration (GSA) offered the first such plan, but the GSA, whose principal mission is the management of physical assets belonging to the government, was not the ideal agency to oversee emergency responses. Following the disaster at the Three Mile Island Nuclear Power Plant in 1979, President James E. Carter issued an executive order creating such an agency, FEMA.

In September 1980, Carter issued another executive order in which he called on FEMA to create a "national contingency plan" that would coordinate federal agencies' responsibilities and authorities in the event of a nuclear accident. FEMA in March 1982 established the Federal Radiological Preparedness Coordinating Committee, which consisted of representatives from federal agencies with responsibilities for responding to radiological emergencies. The purpose of the committee was to coordinate federal planning and preparedness activities, and

to help state and local governments develop their own coordinated plans.

At the same time, FEMA directed the EPA to develop training for state and local officials in areas ranging from decision making to radiation dose assessment. The agency also tasked the Department of Energy (DOE) with putting in place systems for emergency radiation detection and measurement. FEMA also directed DOE to establish a federal radiological monitoring and assistance plan. Together with EPA, NRC, and other agencies, the DOE in the early 1980s developed the Federal Radiological Monitoring and Assessment Center (FRMAC) to implement the plan it developed. DOE maintains the FRMAC, but in the event of an emergency, EPA would assume control in the middle and latter phases of the crisis.

FRERP, other RERPs, and their evolution. The Federal Radiological Preparedness Coordinating Committee completed the FRERP in 1985, and in 1987 the EPA published its own RERP describing how it would support state and local agencies in the event of a radiological emergency. States have also developed their own RERPs. Following the accident at the Chernobyl Nuclear Power Plant in what was then the Soviet Union (now Ukraine) in April 1986, the Federal Radiological Preparedness Coordinating Committee revised the FRERP to include a response to international radiological incidents that could affect the United States.

The revised plan also incorporated responses to smaller situations, such as lost radiation sources or lost radioactive material. EPA was made the lead federal agency in both international and lost-course incidents. In 1989, EPA responded to such a situation, when it was discovered that abandoned materials at the Radium Chemical Company facility in New York City presented a radiological hazard to the neighborhood.

During the 1980s, participating organizations took part in two full-field exercises to prepare for a radiological emergency. In June 1995, President William J. Clinton signed Presidential Decision Directive (PDD) 39, which directed the response of federal agencies to terrorist attack. PDD 39 directed EPA to provide chemical and radiation-related technical support to the Federal Bureau of Investigation in the event of a terrorist incident. Additional directives in 1998 led to a revision of the EPA RERP in 2000.

### ■ FURTHER READING:

#### BOOKS:

Congel, F. J. *Criteria for Preparation and Evaluation of Radiological Emergency Response Plans and Preparedness in Support of Nuclear Power Plants: Criteria for Protective Action Recommendations For Severe Accidents: Draft Report for Interim Use and Comment*. Washington, D.C.: U.S. Nuclear Regulatory Commission/Federal Emergency Management Agency, 1996.

## PERIODICALS:

Muhlebach, Richard. "What's Your Disaster Plan?" *National Real Estate Investor* 44, no. 8 (August 2002): 64.

## ELECTRONIC:

EPA's Radiation Protection Program: Emergency Response. Environmental Protection Agency. <<http://www.epa.gov/radiation/rert/history.htm>> (March 4, 2003).

Federal Radiological Emergency Response Plan. Florida Department of Community Affairs. <<http://www.dca.state.fl.us/bpr/EMTOOLS/Nuclear/frerp.htm>> (March 4, 2003).

## SEE ALSO

*Domestic Emergency Support Team, United States Emergency Response Teams*  
*Environmental Issues Impact on Security*  
*EPA (Environmental Protection Agency)*  
*FEMA (United States Federal Emergency Management Agency)*  
*Nuclear Emergency Support Team, United States*  
*Nuclear Regulatory Commission (NRC), United States*

## Reagan Administration (1981–1989), United States National Security Policy

■ CARYN E. NEUMANN

To Ronald Reagan, national security meant battling the Soviet Union for world supremacy. Much more conservative than his predecessors, Reagan argued that international instability of the world could be traced to Moscow and he insisted that the United States needed to use military force to protect its global interests. As a result of these assumptions, the Reagan administration promoted a massive buildup of both conventional and nuclear weapons to close the gap that it presumed had developed between Soviet and American forces.

Reagan had little foreign policy expertise. A popular actor who had served as governor of California, he won the presidency from Jimmy Carter in large part because he promised to engineer a return to the glory days of international respect for the U.S. To help achieve this goal, Reagan revamped the national security system. Secretary of State Alexander Haig served as the primary advisor on foreign affairs, while National Security Advisor (NSA) William Clark took responsibility for developing, coordinating, and monitoring national security policy.

Reagan made another significant change by terminating the policy of détente with the Soviet Union that had

been pursued by his predecessors. He made this choice out of his expressed belief that the inherent evil of Soviet totalitarianism had created an "evil empire." He repeatedly stated the American resolve to fight communist aggression anywhere in the world. This determination would lead the U.S. to confront communism in Grenada, El Salvador, and Nicaragua, with the latter effort turning into the Iran-Contra scandal.

Reagan's actions were occasionally more moderate than his words and the administration appeared reluctant to be the first since World War II to fail to arrive at an agreement on arms with the Soviets. President Carter had negotiated the SALT II treaty but Reagan believed that it was fatally flawed. While agreeing to abide by the restrictions of the agreement as long as the Soviet Union did the same, Reagan refused to submit it to the Senate for ratification. In 1982, the administration announced the outlines of a replacement arms control treaty. To show displeasure with past agreements that merely reduced the growth of each side's arsenals instead of reducing the total numbers of weapons, the Reagan administration security team named the new arms control plan START (Strategic Arms Reduction Talks). This new arms policy was designed to bring about cuts in total American and Soviet missiles and warheads, but the two sides were unable to reach an agreement.

In 1983, Reagan escalated the nuclear arms race with the Soviet Union by authorizing the Defense Department to develop a Strategic Defense Initiative (SDI). Known to its advocates and critics as "Star Wars," SDI would involve the development of a complex anti-missile defense system employing laser and high-energy particle weapons to destroy enemy missiles in outer space before they reached their targets. By destroying weapons rather than people, SDI would free defense strategy from the concept of mutually assured destruction that had long governed Soviet and American attitudes toward war. Although the system was never built and many scientists doubted that it could ever be constructed in the form proposed, the Soviets felt obligated to keep pace by launching their own SDI-type development program.

By the end of Reagan's presidency, his anti-Soviet rhetoric had cooled. Under Mikhail Gorbachev, the Soviets pursued renewed détente and the Reagan administration responded positively. In 1987, the U.S. and U.S.S.R. signed a treaty to eliminate intermediate range (300 to 3,000 miles) nuclear forces (INF). The agreement marked the first time that the two nations had agreed to destroy an entire class of weapons systems.

Reagan entered the White House with a campaign promise to refurbish American defense capabilities and to regain military superiority over the Soviet Union. He exited the Oval Office after completing a treaty that served as the first step toward the eventual end of the arms race. By redirecting the thrust of national security policy, the Reagan administration is widely credited with winning the Cold War.



In the shadow of an American M-60 tank, two U.S. soldiers stand guard over three Grenadian prisoners. President Ronald Reagan ordered the invasion of Grenada in 1983 in order to oust its Marxist government. AP/WIDE WORLD PHOTOS.

■ FURTHER READING :

BOOKS:

Boll, Michael M. *National Security Planning Roosevelt Through Reagan*. Lexington: University Press of Kentucky, 1988.

Thomson, Kenneth W., ed. *The Reagan Presidency*. Lanham, MD: University Press of America, 1997.

ELECTRONIC:

White House. "History of the National Security Council, 1947–1997." <<http://www.whitehouse.gov/nsc/history.html>> (April 25, 2003).

SEE ALSO

*Cold War (1972–1989): The Collapse of the Soviet Union*  
*Iran-Contra Affair*

*National Security Strategy, United States*  
*START I Treaty*

Real IRA (RIRA)

The Real Irish Republican Army (Real IRA, or RIRA), also known as the True IRA, formed in early 1998 as a clandestine armed wing of the 32-County Sovereignty Movement, a "political pressure group" dedicated to removing British forces from Northern Ireland and unifying Ireland. The 32-County Sovereignty Movement opposed Sinn Fein's adoption in September, 1997, of the Mitchell principles of democracy and nonviolence and opposed

the amendment in December 1999 of Articles 2 and 3 of the Irish Constitution, which laid claim to Northern Ireland. Michael “Mickey” McKeivitt, who left the IRA to protest its cease-fire, leads the group; Bernadette Sands-McKeivitt, his wife, is a founder-member of the 32-County Sovereignty Movement, the political wing of the RIRA.

**Organization activities.** The Real IRA has claimed to have committed or is believed to be responsible for a number of bombings, assassinations, and robberies. Many Real IRA members are former Irish Republican Army (IRA) members who left that organization following the IRA cease-fire and who bring to RIRA a wealth of experience in terrorist tactics and bomb construction. RIRA targets include British military and police in Northern Ireland and Northern Ireland Protestant communities. RIRA is linked to and understood to be responsible for the car bomb attack in Omagh, Northern Ireland, on August 15, 1998, that killed 29 and injured 220 persons. The group began to observe a cease-fire following Omagh but in 2000 and 2001 resumed attacks in Northern Ireland and on the UK mainland against targets such as MI6 headquarters and the BBC.

RIRA’s size is estimated at 100 to 200 activists plus possible limited support from IRA hardliners dissatisfied with the IRA cease-fire and other republican sympathizers. British and Irish authorities arrested at least 40 members in the spring and summer of 2001, including leader McKeivitt, who is currently in prison in the Irish Republic awaiting trial for being a member of a terrorist organization and directing terrorist attacks.

Suspected of receiving funds from sympathizers in the United States and of attempting to buy weapons from U.S. gun dealers, RIRA also is reported to have purchased sophisticated weapons from the Balkans. Three Irish nationals associated with RIRA were extradited from Slovenia to the UK and are awaiting trial on weapons procurement charges.

As of April 2003, the U.S. Department of State no longer listed the IRA as a foreign terrorist organization, but did list the Real IRA. The RIRA operates in Northern Ireland, Irish Republic, and Great Britain.

#### ■ FURTHER READING:

##### ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001. Annual Report: On the Record Briefing. May 21, 2002. <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

#### SEE ALSO

*Terrorism, Philosophical and Ideological Origins*  
*Terrorist and Para-State Organizations*  
*Terrorist Organization List, United States*  
*Terrorist Organizations, Freezing of Assets*

## Reconnaissance

Reconnaissance is a term for efforts to gain information about an enemy, usually conducted before, or in service to, a larger operation. The French word entered the English language in 1810—not coincidentally, at a time when British and other armies were at war with Napoleon’s French forces. Reconnaissance is an important component of military and intelligence activities, as well as civilian undertakings designed to protect the public safety from hazards both natural and manmade.

In the military or espionage environment, reconnaissance can take the form of activities by scouts or other specialists. The use of what would now be called “human intelligence” in a reconnaissance capacity dates back to ancient times, when, according to the Christian Old Testament, 12 spies went into the land of Canaan to scout out the territory. Today, reconnaissance is the work of special units practicing a specialized craft.

Reconnaissance aircraft range from the U-2 and SR-71 Blackbird to the E-2C Hawkeye and P-3 Orion. Additionally, the skies bristle with reconnaissance satellites operated by the U.S. military, the National Security Agency, and military or intelligence services of other nations. Even some seagoing craft, most notably submarines, can serve a reconnaissance function.

The major reconnaissance components of the U.S. intelligence community are the National Reconnaissance Organization and the National Imagery and Mapping Agency. In the civilian realm are meteorological services such as the National Oceanic and Atmospheric Administration, which makes extensive use of reconnaissance technology to map and forecast weather patterns. Additionally, the Department of Energy, Environmental Protection Agency, and other organizations conduct reconnaissance for radiological hazards and other forms of danger.

#### ■ FURTHER READING:

##### BOOKS:

Burrows, William E. *By Any Means Necessary: America’s Secret Air War in the Cold War*. New York: Farrar, Straus and Giroux, 2001.

Day, Dwayne A., and John M. Logsdon. *Eye in the Sky: The Story of the Corona Spy Satellites*. Washington, D.C.: Smithsonian Institution Press, 1998.

Gann, Ernest. *The Black Watch: The Men Who Fly America's Secret Spy Planes*. New York: Random House, 1989.

Osborn, Shane, and Malcolm McConnell. *Born to Fly: The Untold Story of the Downed American Reconnaissance Plane*. New York: Broadway Books, 2001.

#### ELECTRONIC:

National Imagery and Mapping Agency. <<http://www.nima.mil/>> (April 1, 2003).

National Reconnaissance Office. <<http://www.nro.gov/>> (April 1, 2003).

#### SEE ALSO

*Balloon Reconnaissance, History*

*E-2C*

*NIMA (National Imagery and Mapping Agency)*

*NRO (National Reconnaissance Office)*

*P-3 Orion Anti-Submarine Maritime Reconnaissance Aircraft*

*Photographic Interpretation Center (NPIC), United States National*

*Photography, High-Altitude*

*Satellites, Spy*

## Red Brigades.

SEE *Anti-Imperialist Territorial Nuclei (NTA)*.

## Red Code

Red was a Japanese naval code created during World War I and used until the outbreak of World War II. The Red code used the additive encryption method. The code assigned words and syllables numerical values. Before transmissions, these numbers were encrypted a second time using an additive codebook. The book contained a series of numbers that were added to the original numerical message in sequence. Each message contained a key that told the receiver where to begin the additive sequence in the book to decode the message. Cryptologists named the code Red after the color of the folder in which deciphered codes were bound.

In 1923, a United States Navy intelligence officer located a copy of the 1918 Imperial Japanese Navy secret operating code in the luggage of a visiting Japanese attaché. The codebook was clandestinely photographed and a special cryptology unit, known as the Research Desk, was created to begin the task of monitoring and deciphering intercepted messages. At the time, U.S. Naval Intelligence monitored only ship-to-ship communications and some radio transmissions in Asia and the Pacific. The Research Desk team established intercept stations throughout the Pacific and increased monitoring of Japanese diplomatic and military transmissions.

Cryptologists worked for five years to fully translate and break Red, the additive cipher that the 1918 codebook contained. Intercepts continued to use the aging code, facilitating the work of U.S. code breakers. In 1926, Lieutenant Joseph J. Rochefort accepted the directorship of the Research Desk. Rochefort was a skilled code breaker, but also fluent in the Japanese language and undertook much of the translation work for Red himself. Repeated messages and phrases that appeared in several transmissions helped code breakers recognize various additive decipherments. Three years after the analysis of Red began, cryptologist Agnes Meyer Driscoll cracked the code's additive encryption key. With the additive key, and the photographs of the original code book, any Red code message could be deciphered.

The Japanese replaced Red with a more sophisticated code on December 1, 1930. However, the new code, called Blue, contained numeric patterns that so closely resembled Red that Driscoll and her team were able to decipher and translate Blue in only two years.

#### ■ FURTHER READING:

##### BOOKS:

Budiansky, Stephen. *Battle of Wits: The Complete Story of Codebreaking in World War II*. New York: Touchstone Books, 2002.

Matthews, Tony. *Shadows Dancing: Japanese Espionage Against the West*. New York: St. Martin's Press, 1993.

##### SEE ALSO

*Purple Machine*

*World War II, United States Breaking of Japanese Naval Codes*

## Red Hand Defenders (RHD)

Red Hand Defenders (RHD) is an extremist terrorist group formed in 1998 and composed largely of Protestant hardliners from loyalist groups observing a cease-fire. RHD seeks to prevent a political settlement with Irish nationalists by attacking Catholic civilian interests in Northern Ireland. In July, 2001, the group issued a statement saying it considered all nationalists "legitimate targets." RHD is a cover name often used by elements of the banned Ulster Defense Association and the Loyalist Volunteer Force. In recent years, the group has carried out numerous pipe bombings and arson attacks against "soft" civilian targets such as homes, churches, and private businesses, including a bombing outside a Catholic girls school in North Belfast. RHD claimed responsibility for the car-bombing murder in March, 1999, of Rosemary Nelson, a prominent Catholic nationalist lawyer and human rights

campaigner in Northern Ireland, and for the murder of a Catholic journalist in September, 2001.

The RHD may have up to 20 members acting in Northern Ireland, some of whom have considerable experience in terrorist tactics and bombmaking.

#### ■ FURTHER READING:

##### ELECTRONIC:

CDI (Center for Defense Information), Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <<http://www.cdi.org/terrorism/terrorist.cfm>> (April 17, 2003).

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001." Annual Report: On the Record Briefing. May 21, 2002. <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

#### SEE ALSO

*Terrorism, Philosophical and Ideological Origins*  
*Terrorist and Para-State Organizations*  
*Terrorist Organization List, United States*  
*Terrorist Organizations, Freezing of Assets*

stealing documents and radio equipment. Red Orchestra agents infiltrated the German military intelligence Abwehr headquarters in Paris and successfully tapped its phones. This permitted agents to intercept intelligence information transmitted directly from Berlin.

The greatest espionage achievement of the organization, however, was that of the Swiss ring, nicknamed Lucy. The Red Orchestra unit received leaked information and a document relating to the Nazi plan to invade the Soviet Union. These documents, which included the proposed date for the launch of the offensive, were turned over to the Soviet army and government, but were wholly ignored.

Trepper's network began to crumble in 1942, when several Red Orchestra agents were arrested in Belgium. Later that year, the Gestapo tracked down Trepper himself and arrested him in Paris. The Gestapo managed to find and eliminate many Red Orchestra agents. Some rings continued to operate throughout the war, but on a smaller scale. Trepper escaped his Nazi captors and tried to rebuild his group, but by 1944 the Red Orchestra network had been largely dissolved.

#### ■ FURTHER READING:

##### BOOKS:

Tarrant, V. E. *The Red Orchestra, the Soviet Spy Network Inside Nazi Europe*. New York: Bantam, 1996.

## Red Orchestra

The Red Orchestra was the name given to a network of communist, Soviet-affiliated spies during World War II. The group provided intelligence to the Soviet government, but also functioned as a resistance organization against the Nazis. During its three years in operation, the Red Orchestra smuggled key German secrets and documents to Allied forces, and rescued several political prisoners, mostly communist dissidents.

Leopold Trepper, a Polish-born Jew and communist activist, joined the Soviet Red Army Intelligence Service in the mid-1930s. He was later assigned to the Peoples Commissariat for Internal Affairs (NKVD), a fledgling Soviet secret police and espionage agency. Before World War II began in Europe, Trepper established a network of communist sympathizers and leftist political activists. When the war began in 1939, Trepper turned his network into a spy ring, bent on gathering Nazi secrets and other intelligence useful to the Soviet army.

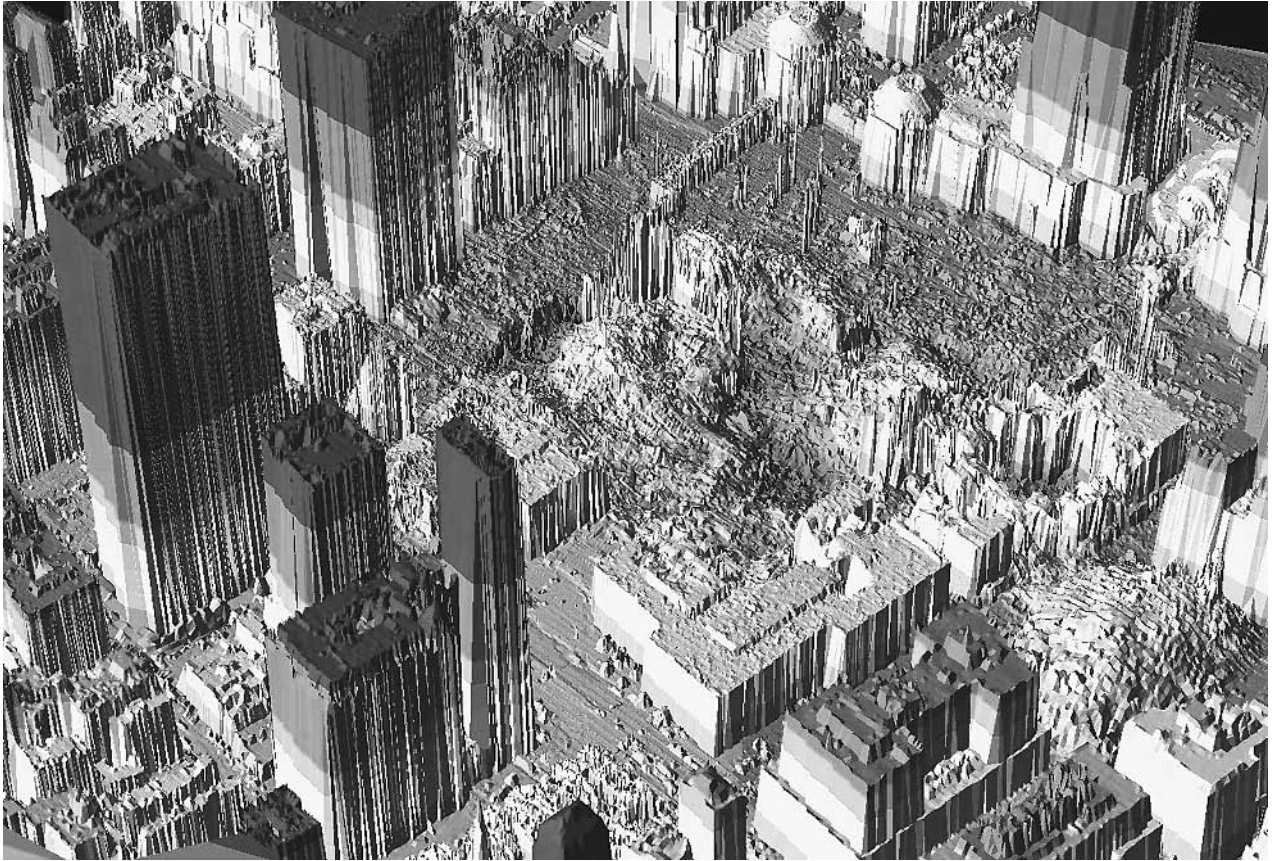
Trepper's network, the Red Orchestra, soon had operating divisions, or rings, in Nazi occupied France, Belgium, Holland, and neutral Switzerland. Each ring had varying successes. The French unit provided information to Resistance fighters and infiltrated several Nazi offices in Paris,

## Remote Sensing

#### ■ WILLIAM C. HANEBERG

Remote sensing is the acquisition of information about an object or phenomenon by a device located a considerable distance from the object or phenomenon. The term was coined in the mid-1950s by an Office of Naval Research scientist to distinguish the information obtained from the first generation of meteorological satellites from that which had been traditionally obtained by airplane-based aerial photography. In practice, however, information obtained from high-flying reconnaissance aircraft such as the U-2 and SR-71 can also be considered to be a product of remote sensing.

In addition to providing panchromatic (black and white) and multispectral color images that resemble photographs, some modern remote sensing satellites contain hyperspectral sensors that record information using dozens or hundreds of reflected electromagnetic energy wavelength bands that extend beyond the range of human vision. The simplest kind of multispectral image consists of red, blue, and green bands added together to form a color composite image. Image processing software can be used, particularly with hyperspectral data, to identify the chemical composition of rocks, vegetation type, soil or



This LIDAR photo shows elevations at the World Trade Center site in New York on September 19, 2001. LIDAR is short for Light Detection and Ranging, a remote sensing technique. ©AFP/CORBIS.

water pollution, and other attributes that can be characterized in terms of spectral reflectance. Paired images can also be used to stereoscopically construct digital elevation models (DEMs), which can subsequently be transformed into topographic maps or three dimensional terrain models from space.

Other satellites contain active sensors that generate their own electromagnetic signals and record the reflections rather than passively recording reflected natural radiation. Synthetic aperture radar (SAR), in particular, is a useful tool because it can penetrate clouds and be used at night. The length of a radar antenna is known as its aperture and, in general, the resolution of a radar image is proportional to antenna length. The term synthetic aperture refers to a technique in which the constant movement of a satellite is combined with periodic radar pulses and computer processing to achieve the same effect as would be obtained by using a very large antenna. Pairs of SAR images can be combined to produce interferometric (InSAR) images that portray millimeter to centimeter scale changes in the elevation of Earth's surface. InSAR is becoming an increasingly important tool for monitoring tectonic movements of Earth's crust, subsidence associated with heavy groundwater pumping, and other geologic processes. It

can also be used to construct digital elevation models. Another active source remote sensing technique is light detection and ranging (LIDAR), which is similar to radar but uses a laser instead of radio waves to produce extremely detailed topographic maps and images.

It is generally understood that remote sensing satellites must have a resolution of 5 meters (m) or less to be useful for intelligence work. The Landsat 1 satellite, launched by the United States in 1972 and from which imagery was freely available, had a resolution of 80 m. Landsat 7, launched in 1999 and still in service, has resolutions of 15 m for panchromatic images, 30 m for its six multispectral bands, and 60 m for its thermal band. The French SPOT 5 satellite offers commercially available images ranging in resolution from 5 m for panchromatic to 20 m for infrared. Publicly available images with these coarse resolutions are useful for such tasks as delineating large-scale geologic features, evaluating inaccessible or denied terrain, examining land use patterns, and inferring levels of crop stress, but not for detailed intelligence work. In recent years, however, commercial remote sensing satellites have been able to obtain high-resolution images that are of intelligence quality. The commercial QuickBird satellite launched from Vandenberg Air Force Base in late

2001, for example, provides commercially available imagery with 61 cm panchromatic and 2.44 m multispectral resolution. The commercial IKONOS satellite, launched in 1999, can produce 1 m resolution color images.

Even the best publicly available imagery does not approach the resolution provided by classified intelligence satellites. The earliest KeyHole intelligence satellites (KH1 series), the first of which was launched by the United States in 1960, had a resolution of 2 m. Photographic film from KeyHole satellites was recovered using film drops until 1972, when digital imaging and transmission were instituted. The KH12 series is estimated to have a resolution of approximately 2 cm, although no images with this resolution have been released. Intelligence-quality images with sub-meter resolution can be used to assess details of troop or materiel movement, the progress of construction projects, and war damage in denied or otherwise inaccessible areas. Perhaps the most widely known application of remotely sensed images for intelligence work was the use of satellite and U-2 airplane photographs to detect the presence of Russian missiles in Cuba, which led to the 1962 Cuban missile crisis.

#### ■ FURTHER READING:

##### BOOKS:

Campbell, James B. *Introduction to Remote Sensing, 3rd ed.* New York: Guilford Press, 2002.

##### ELECTRONIC:

Hardin, R. Winn. "Remote Sensing Satellite Market Pits Industry Against U.S. Policy." OE Reports. May 1999. <<http://www.spie.org/app/publications/magazines/oerarchive/may/may99/cover1.html>> (November 14, 2002).

Short, Nicholas M., Sr. "The Remote Sensing Tutorial." NASA. October 22, 2002. <<http://rst.gsfc.nasa.gov/>> (November 14, 2002).

Skorve, Johnny E. "Using Satellite Imagery to Map Military Bases of the Former Soviet Union." Earth Observation Magazine. April 2002. <<http://www.eonline.com/Common/currentissues/Apr02/skorve.htm>> (November 14, 2002).

International Society for Photogrammetry and Remote Sensing, Department of Geomatic Engineering, University College London, Gower Street, London WC1E 6BT, United Kingdom. 44 207679 7226. <<http://www.isprs.org/>> (November 14, 2002).

##### SEE ALSO

*Bomb Damage, Forensic Assessment Cameras*  
*Cuban Missile Crisis*  
*Electromagnetic Spectrum*  
*Electro-optical Intelligence*  
*Geospatial Imagery*  
*LIDAR (Light Detection and Ranging)*  
*Photographic Resolution*  
*Photography, High-Altitude*  
*RADAR, Synthetic Aperture*

*U-2 Spy Plane*  
*Unmanned Aerial Vehicles (UAVs)*

## Remote Sentinels.

SEE *Biological Input/Output Systems (BIOS)*.

## Retina and Iris Scans

■ AGNIESZKA LICHANSKA

The retina is the neural part of the eye responsible for vision and the pattern of blood vessels serving the retina is as unique as a fingerprint.

The technology that scans the retina is known as retinal scanning. The true target for the scan is the capillary pattern in the retina. The process relies on generating images of the retina using a low-intensity light source. In the 1930s retinal capillary patterns were suggested to be unique, but the technology used to exploit this information was developed much later. Although military and high-security use of photographic retinal scans began decades earlier, by 1985, retinal scan technology became available for computerized biometric identification and commercial security use.

Retinal scans are just one of the biometric methods using the eye for personal identification. Two years after the first retinal scanner was developed in 1987, Leonard Flom and Aram Safir patented the use of the iris as a personal identifier. However, it was not until 1994 when John Daugman developed the technology for iris scanning that it became useful, and since then iris scanning has begun to challenge the retinal scans. Currently a number of companies claiming that they perform retinal scanning, in reality are performing iris scans.

**Retina scanning procedures.** Retinal scans are based on the presence of the fine network of capillaries supplying the retina with oxygen and nutrients. These vessels absorb light and can be easily visualized with proper illumination. Retinal scans require close contact of user and scanner, a perfect alignment of the eye with a scanner, and no movement of the eye. The examiner is required to keep the subject's eye within half an inch of the instrument. The subject must focus on a pinpoint of little green light (to properly align the eye) and avoid blinking. A low-intensity coherent light is then transmitted through the eye and the reflected image of the retinal capillary pattern is recorded by the computer.





An executive demonstrates a retinal scanner used for identification at the International Air Transport Association security symposium in Atlanta in 2001. AP/WIDE WORLD PHOTOS.

Although retinal patterns are generally thought to be constant during a person's life, they can change in case of diabetes, glaucoma, retinal degenerative disorders or cataracts. Therefore, although retinal scans are nearly 100% accurate they cannot be used as a universal security measure without making allowances for normal changes.

An initial scan (enrollment) takes a minimum of five scans and lasts approximately 45 seconds; subsequent authentication scans are faster and take only 10–15 seconds. An acquired image containing 320–400 reference points is converted to a map of the retina and used to identify a match from the templates encoded in the scanner's software. Retinal images captured are extremely small, only 35 bytes in size.

**Retinal scans versus iris scans.** Retinal scans are considered to be too intrusive for a general security use and the prolonged exposure to light emitted by the scanners might

be harmful to the eye. As a result a strong competition to the retinal scans was launched by iris scanning technology. The number of companies offering iris scanning are increasing. The main reason is the fact that the iris is also unique and offers high confidence in identification. There is only a chance of one in  $10^{78}$  that two irises will be identical.

Iris scans use the characteristics more similar to fingerprints than to the retinal vein pattern. The colored part of the eye appears to be as unique as fingerprints and retina. Scanning technology takes advantage of crypts, furrows, ridges, striations, ligaments, and collarette. While 240 points are recorded, the image size is 512 bytes, over ten times larger than a retinal scan. The main advantage of the iris scans is the ability to perform them from a distance of up to three feet and short time of scan of only 20 seconds initially, with subsequent identification requiring only two seconds. Glasses and contact lenses do not interfere with the scanning process and identification.

**Scanners.** The technology for retinal scans has changed in recent years. The initial large devices are now being replaced by smaller and more accurate instruments. The first commercial retinal scanner was developed by EyeDentify in 1984 with the launch of the Eyedentification 7.5 personal identification unit. One of the most recent developments in the area is a small mobile and easy to use retinal scanner developed by Retinal Technologies from Boston. Although it was initially developed for diagnostic purposes it will be available as a security tool as well.

Fooling the retinal scanner is very difficult, as they require intact retinas to complete a scan. Following death, the retina degrades very quickly and thus cannot be used in most cases for accurate post-mortem identification. Although often a popular movie special effect, using a retina detached from a cadaver would fail to pass notice by modern scanning equipment. Likewise, surgical alteration of the retinal pattern would be not only a dangerous and extremely expensive process, but the changes introduced would be readily detected by modern scanning equipment.

In contrast to the retinal scanners, iris scanners are of two main types: active and passive. The active system works from 3 to 14 inches and also requires the user to move forward and backwards so the camera is adjusted properly. In contrast the passive system can work over longer distances one to three feet. The main technology developer is Iridian Technologies, which holds the patents to the concepts and technologies involved.

**Security uses of retinal and iris scans.** Biometric techniques are used in identification and authentication. The features used for the two processes can overlap or can be different. Authentication requires high accuracy to ensure restricted access. Retinal and iris scans offer high accuracy, and the primary users of retinal scans are military and government facilities, such as CIA, FBI, and NASA. Scans are used to control access to high security areas. The technology is currently spreading beyond these institutions and is being used by Cook County Prison in Illinois (to ensure the identity of the prisoners) as well as General Dynamics (a defense contractor).

Some of the Japanese banks use retinal scans in ATM machines to prevent unauthorized use of the system. Trials in the USA with biometric ATM security are using iris recognition systems instead. However, in Illinois retinal scans in conjunction with fingerprinting are used to prevent welfare fraud.

Acceptance is growing for the iris recognition systems and they are now used by government agencies, commercial companies, and in the public sector. Among the government users are the U.S. Congress and the Departments of Defense, State and Treasury. Commercial companies that protect themselves by using iris recognition include Bank United, GTE, Hewlett Packard, Lockheed Martin, and British Telecom. Other places with restricted access areas, including airports, have acquired scanning

technologies in the wake of the September 11, 2001, terrorist attacks upon the United States. Scanning technology systems were recently installed at Charlotte (North Carolina), Amsterdam (Netherlands) and Frankfurt (Germany) mainly for security purposes to check the employees and provide controlled access to the secure areas of the airports. Studies are underway to test if scanning technologies can be used to facilitate rapid check in and to streamline border crossing. The Schipol Airport in Amsterdam is one of the most recent airports to test the iris recognition system. The details of an individual's iris are stored on a special card and a subsequent check-in is performed by a simple iris scan to confirm identity. Eight of the largest Canadian airports (Toronto, Vancouver, Ottawa, Montreal, Halifax, Winnipeg, Calgary and Edmonton) plan to install similar systems by the end of 2003.

Scanning is also becoming part of security measures for sports and entertainment venues. For example, organizers at the 2002 Sydney Olympics used an iris scanning system termed EyeTicket. Use of retinal scans outside the high security areas is, in many areas, being replaced by iris scanning, which is easier to perform, is less intrusive for the user, and provides adequately accurate identification.

#### ■ FURTHER READING:

##### BOOKS:

- Ashbourn, Julian. *Advanced Identity verification. The complete guide.* London: Springer Verlag, 2000.
- Nanavati, Samir, Michael Thieme, and Raj Nanavati. *Biometrics: Identity Verification in a Networked World.* New York: Wiley and Sons, 2002.

##### PERIODICALS:

- French, M. "Retinal eyes biometric security. Company reveals its scanning technology." *Mass High Tech, The Journal of New England Technology*, 32 (2001).

##### ELECTRONIC:

- DORO Inc. <<http://www.dorosecurity.com/index2.html>> (14 December 2002).
- Court Technology Laboratory. "Biometrics and the Courts. Individual biometrics." <<http://ctl.ncsc.dni.us/>> (14 December 2002).
- Find Biometrics. The complete biometrics resource guide for identification and verification. <<http://www.findbiometrics.com/index.html>> (14 December 2002).
- Global Analytic Information Technology Services. "Retinal scanning." <[http://www.gaits.com/biometrics\\_retinal.asp](http://www.gaits.com/biometrics_retinal.asp)> (14 December 2002).
- IridianTech. <<http://www.iridiantech.com.>> (14 December, 2002).

##### SEE ALSO

*Biological and Biomimetic Systems*  
*Biomedical Technologies*

## Revolutionary Armed Forces of Colombia (FARC)

The Revolutionary Armed Forces of Colombia (FARC) was established in 1964 as the military wing of the Colombian Communist Party. FARC is Colombia's oldest, largest, most capable, and best-equipped Marxist insurgency. FARC is governed by a secretariat, led by Manuel Marulanda (a.k.a. "Tirofijo") and six others, including senior military commander Jorge Briceño (a.k.a. "Mono Jojoy"). FARC is organized along military lines and includes several urban fronts. In 2001, the group continued a slow-moving peace negotiation process with the Pastrana administration that has gained the group several concessions, including a demilitarized zone used as a venue for negotiations.

**Organization activities.** FARC is responsible for bombings, murder, kidnapping, extortion, hijacking, as well as guerrilla and conventional military action against Colombian political, military, and economic targets. In March, 1999, FARC executed three U.S. Indian rights activists on Venezuelan territory after kidnapping them in Colombia. Foreign citizens often are targets of FARC kidnappings for ransom. The group has well-documented ties to narcotics traffickers, principally through the provision of armed protection.

FARC has approximately 9,000 to 12,000 armed combatants and an unknown number of supporters, mostly in rural areas. FARC operates in Colombia with some activities in Venezuela, Panama, and Ecuador, while Cuba provides FARC some medical care and political consultation.

### ■ FURTHER READING :

#### ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001. Annual Report: On the Record Briefing. May 21, 2002. <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

#### SEE ALSO

*Terrorism, Philosophical and Ideological Origins  
Terrorist and Para-State Organizations*

## Revolutionary Nuclei

Revolutionary Nuclei (RN) (also known as Revolutionary Cells) emerged from a broad range of antiestablishment and anti-U.S./NATO/EU leftist groups active in Greece between 1995 and 1998. The group is believed to be the successor to or offshoot of Greece's most prolific terrorist group, Revolutionary People's Struggle (ELA), which, as of mid-2002, had not claimed an attack since January 1995. Indeed, RN appeared to fill the void left by ELA, particularly as lesser groups faded from the scene. RN's few communiqués show strong similarities in rhetoric, tone, and theme to ELA proclamations. RN claimed an attack in November, 2000.

**Organization activities.** Beginning operations in January 1995, RN has claimed responsibility for some two dozen arson attacks and bombings against a range of U.S., Greek, and other European targets in Greece. In its most infamous and lethal attack to date, the group claimed responsibility for a bomb it detonated at the Intercontinental Hotel in April 1999 that resulted in the death of a Greek woman and injured a Greek man. RN's *modus operandi* includes warning calls about impending attacks, attacks targeting property rather than individuals; use of rudimentary timing devices; and strikes during the late evening to early morning hours. RN last attacked U.S. interests in Greece in November 2000 with two separate bombings against the Athens offices of Citigroup and the studio of a Greek-American sculptor. The group also detonated an explosive device outside the Athens offices of Texaco in December 1999. Greek targets have included court and other government office buildings, private vehicles, and the offices of Greek firms involved in NATO-related defense contracts in Greece. Similarly, the group has attacked European interests in Athens, including Barclays Bank in December 1998 and November 2000.

RN membership is believed to be small, probably drawing from the Greek militant leftist or anarchist milieu. The RN's primary area of operation is in the Athens metropolitan area, and it is assumed to be a self-sustaining organization.

### ■ FURTHER READING :

#### ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001. Annual Report: On the Record

Briefing. May 21, 2002. <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

SEE ALSO

*Terrorism, Philosophical and Ideological Origins*  
*Terrorist and Para-State Organizations*  
*Terrorist Organization List, United States*  
*Terrorist Organizations, Freezing of Assets*

SEE ALSO

*Terrorism, Philosophical and Ideological Origins*  
*Terrorist and Para-State Organizations*  
*Terrorist Organization List, United States*  
*Terrorist Organizations, Freezing of Assets*

## Revolutionary Organization 17 November (17 November)

The Revolutionary Organization 17 November (a.k.a. 17 November) is a radical leftist group established in 1975 and named for the student uprising in Greece in November, 1973, in protest of the military regime. Seventeen November has an agenda that is anti-Greek establishment, anti-U.S., anti-Turkey, anti-NATO, committed to the ouster of U.S. bases, removal of Turkish military presence from Cyprus, and the severing of Greece's ties to NATO and the European Union (EU).

**Organization activities.** Seventeen November's initial attacks were assassinations of senior U.S. officials and Greek public figures. The group added bombings in the 1980s and, since 1990, has expanded targets to include EU facilities and foreign firms investing in Greece. Seventeen November adherents are known to use improvised rocket attacks. In June, 2000, 17 November claimed responsibility for the murder of British Defense Attaché Stephen Saunders.

Operating in or near Athens, Greece, the exact size of 17 November is unknown, but membership is presumed to be limited to a small cadre.

■ FURTHER READING:

ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001. Annual Report: On the Record Briefing. May 21, 2002. <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

## Revolutionary People's Liberation Party/ Front (DHKP/C)

The Revolutionary People's Liberation Party/Front (DHKP/C) was originally formed in 1978 as Devrimci Sol, or Dev Sol, a splinter faction of the Turkish People's Liberation Party/Front. Renamed in 1994 after factional infighting, it espouses a Marxist ideology and is virulently anti-U.S. and anti-NATO. The organization finances its activities chiefly through armed robberies and extortion. It also operates as, or is known as Devrimci Sol, Revolutionary Left, and Dev Sol.

**Organization activities.** Since the late 1980s, the DHKP/C has concentrated attacks against current and retired Turkish security and military officials. The group began a new campaign against foreign interests in 1990. DHKP/C adherents assassinated two U.S. military contractors and wounded a U.S. Air Force officer to protest the Gulf War. The group launched rockets at the U.S. Consulate in Istanbul in 1992. In early 1996, the group assassinated a prominent Turkish businessman and others, its first significant terrorist acts as DHKP/C. Turkish authorities thwarted DHKP/C attempts in June, 1999, to fire light antitank weapons at the U.S. Consulate. DHKP/C conducted its first suicide bombings, targeting Turkish police, in January and September 2001. A series of safehouse raids and arrests by Turkish police over the last few years have weakened the group significantly.

The exact membership in the Revolutionary People's Liberation Party/Front is unknown. DHKP/C conducts attacks in Turkey, primarily in Istanbul, and raises funds in Western Europe.

■ FURTHER READING:

ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001. Annual Report: On the Record

Briefing. May 21, 2002. <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

SEE ALSO

*Terrorism, Philosophical and Ideological Origins Terrorist and Para-State Organizations Terrorist Organization List, United States Terrorist Organizations, Freezing of Assets*

## Revolutionary Proletarian Initiative Nuclei (NIPR)

Revolutionary Proletarian Initiative Nuclei (NIPR) is a clandestine leftist extremist group that appeared in Rome in 2000. NIPR adopted the logo of the Red Brigades of the 1970s and 1980s—an encircled five-point star—for their declarations. NIPR opposes Italy’s foreign and labor policies and claimed responsibility for the bomb attacks in April, 2001, on a building housing a U.S.-Italian-relations association and on an international affairs institute in Rome’s historic center. NIPR claimed to have carried out a May, 2000, explosion in Rome at an oversight committee facility for implementation of the law on strikes in public services as well as an explosion in February, 2002, on the Via Palermo adjacent to the Interior Ministry in Rome.

Comprising about a dozen members, NIPR operates mainly in Rome, Milan, Lazio, and Tuscany.

■ FURTHER READING:

ELECTRONIC:

CDI (Center for Defense Information), Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <<http://www.cdi.org/terrorism/terrorist.cfm>> (April 17, 2003).

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. “Patterns of Global Terrorism 2001.” Annual Report: On the Record Briefing. May 21, 2002. <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

SEE ALSO

*Terrorism, Philosophical and Ideological Origins Terrorist and Para-State Organizations*

*Terrorist Organization List, United States Terrorist Organizations, Freezing of Assets*

## Revolutionary United Front (RUF)

Revolutionary United Front (RUF) is a loosely organized guerrilla force seeking to retain control of the lucrative diamond-producing regions of Sierra Leone. The group funds itself largely through the extraction and sale of diamonds obtained in areas of Sierra Leone that it controls. During 2001, reports of serious abuses by the RUF declined significantly. The resumption of the government’s Disarmament, Demobilization, and Reintegration program in May was largely responsible. From 1991 to 2000, the group used guerrilla, criminal, and terror tactics, such as murder, torture, and mutilation, to fight the government, intimidate civilians, and keep U.N. peacekeeping units in check. In 2000, they held hundreds of U.N. peacekeepers hostage until their release was negotiated, in part, by the RUF’s chief sponsor, Liberian president Charles Taylor. The group also has been accused of attacks in Guinea at the behest of President Taylor.

RUF’s strength is estimated at several thousand supporters and sympathizers who operate in Sierra Leone, Liberia, and Guinea. A UN experts panel report on Sierra Leone asserted that President Charles Taylor of Liberia provided support and leadership to the RUF. The UN has identified Libya, Gambia, and Burkina Faso as conduits for weapons and other materiel for the RUF.

■ FURTHER READING:

ELECTRONIC:

CDI (Center for Defense Information), Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <<http://www.cdi.org/terrorism/terrorist.cfm>> (April 17, 2003).

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. “Patterns of Global Terrorism 2001,” Annual Report: On the record briefing. May 21, 2002 <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17,2003).

U.S. Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

SEE ALSO

*Terrorism, Philosophical and Ideological Origins*

*Terrorist and Para-State Organizations*  
*Terrorist Organization List, United States*  
*Terrorist Organizations, Freezing of Assets*

## Revolutionary War, Espionage and Intelligence

■ ADRIENNE WILMOTH LERNER

The American Revolution officially began with the signing of the Declaration of Independence on July 4, 1776. However, the conflict between Britain and the American colonies escalated to full-scale war from several orchestrated acts of subversion against British authority. High taxation, shipping restrictions, controls on employment and land ownership, as well as lack of representation in British government prompted resistance to British laws by American colonial citizens. The first shots of the Revolution are said to be those that occurred during the Boston Massacre, the British armed retribution for acts of sabotage against British interests, including the events of the Boston Tea Party. The conflict ended with the Treaty of Paris in 1783, granting international recognition for the newly independent United States. The Revolution marked the beginning of a new era in international politics, shifting the world balance of power and military might over the next 230 years.

### Formation of the United States Intelligence Community

At the outbreak of war, the fledgling American government had few resources, and was still divided by the competing interests of rival colonies. Many leaders were suspicious of establishing permanent, national militaries. The American colonies had to recruit volunteers, train, and arm soldiers, a daunting task for the new nation. Colonial militias aided in training soldiers, and at the outbreak of the war, American military command decided to use their more limited forces in guerilla attacks against the stronger, more formalized British army.

In addition to troop strength and weaponry, the British had the significant advantage of having a developed strategic intelligence force within its military corps. The British established a network of Loyalist spies and informants, many of whom were able to infiltrate and report on American military formation, tactics, battle plans, and defensive positions. This espionage gave Britain a decided upper hand in the early months of the conflict, with devastating effect on the American armies.



A statue of Nathan Hale, a revolutionary soldier who was captured and hung by the British for espionage, in front of the Tribune Tower, in Chicago, Illinois. ©SANDY FELSENTHAL/CORBIS.

Before the outbreak of the Revolution, the American colonial government, the Continental Congress, created the Committee of Correspondence in 1775. The purpose of the committee was to establish foreign alliances and gain the aid of foreign intelligence resources. The original intent of the committee was to facilitate the sharing of information about British colonial policy, but at the start of the Revolution, the Committee seized and combed mail for vital intelligence information. The organization was renamed the Committee of Secret Correspondence, and then the Committee of Foreign Affairs, and employed trusted Patriot sympathizers in Britain to feed American leaders intelligence information. After establishing protocol for obtaining information, the committee established a network of couriers to disperse information to battlefield commanders and key government officials. The committee also sought the aid of French forces in the war effort.

The Second Continental Congress also established the Secret Committee. This clandestine committee arranged for American privateers to purchase and smuggle arms to the United States. The committee used large sums of money to pay for weapons, and additionally solicited aid from Britain's numerous European rivals. The world of the Secret Committee began in 1775, amassing weapons while still under British rule. After the Declaration of Independence was signed, the committee burned its papers

and transaction ledgers to protect their contacts in case the colonies lost their bid for sovereignty.

The smuggling of weapons proved a successful venture. The United States armed its troops within months, although supplies remained limited throughout the course of the war. Many American leaders, including Thomas Jefferson, ran successful privateering ventures, using their wealth and diplomatic contacts abroad to smuggle arms for the war effort. American privateers ran their illegal cargo through the British blockade under the guise of foreign named vessels and foreign flags. Patriot spies also learned the new British semaphore code, enabling blockade runners to falsely identify themselves as British ships.

The first United States counterintelligence operations were directed by the Commission for Detecting and Defeating Conspiracies. The commission endowed several groups, mostly in New York and Philadelphia, with the task of apprehending British spies. The organization was the nation's first secret service, employing local militia under its command to help ferret out suspected traitors and enemy spies. The group used the criteria defined by the Committee on Spies when identifying, trying, and sentencing suspects. The rules of the committee, incorporated into the Articles of War in 1776, defined the crimes of treason and espionage during the course of war, and shaped the American intelligence community with its strict definitions of intelligence information, espionage acts, conspiracy, and aiding the enemy.

## Espionage

Although the secret committees of the Second Continental Congress were the first national organizations to address intelligence issues, individuals and civilian spy networks carried out the most vital American intelligence operations of the Revolutionary War.

Robert Townsend used his position as a prominent merchant in British-occupied New York to gather intelligence information on behalf of the American government. Townsend operated a significant spy ring, known as the Culper Ring. The ring employed both men and women, and based its operations in New York and Long Island. Most members of the espionage group used their professions as cover, relying on customers and patrons from the British military to divulge information about British military operations voluntarily. Several members of the Culper Ring were caught by British occupation authorities, but the ring never stopped feeding information to American authorities during the war.

Major John Clark established and administered a similar espionage group in Philadelphia. Clark and his group fed General George Washington critical information and supplies while his troops wintered at Valley Forge. The Clark Ring obtained detailed information about British defenses, supply lines, and battle plans, allowing

the American Patriot forces to plan a series of successful surprise attacks, breaking the British stronghold in the region and paving the way to seize control of Philadelphia.

Several other Patriot civilian espionage rings operated across the country and in Britain. Individual civilians most often contributed to counterintelligence measures by posing as Loyalists and infiltrating British-sympathizing groups. Enoch Crosby and John Honeyman both infiltrated several pro-British organizations and delivered valuable intelligence information about the planned use of Hessian mercenaries in British military operations.

Within the military, espionage operations were often tailored to fit the strategic needs of the battlefield. Scouts, many of whom were American Indians, reported on the location and strength of British military installations and encampments. The first recorded American military agent of espionage was Nathan Hale. After a crushing defeat at the Battle of Long Island, Washington called for a volunteer to spy on the British and report to the American command with details of future battle plans. Hale volunteered, but was later captured behind enemy lines and hanged.

**Covert actions and special operations.** Most American, government-backed espionage actions against the British were covert, strategic operations of deception or sabotage. Blockade running was of critical importance to the American war effort. Though British ships clogged United States harbors, American privateers successfully ran British blockades to provide troops with supplies, ammunition, and even supporting troops from France.

The American government, usually through diplomats abroad, employed a number of agents to sabotage wartime industries in Britain. Munitions factories, shipyards, and weapons storage facilities were the main targets of Patriot sabotage. Twelve separate targets were attacked in London and Portsmouth in a three-year period by one American saboteur before the agent fell into British custody and was executed.

Some operations of deception were more insidious. British troops, wanting to keep some local Indian populations from joining the American cause, bribed village leaders with gifts of blankets and jewelry. Earlier, they gave the Indians blankets from their military sick wards, often infected with smallpox. The disease continued to devastate the American Indian population during the course of the war. Both British and American military personnel traded contaminated goods through Indian trade networks, hoping the goods would fall into enemy hands.

**Codes, cryptology, and secret writing.** American and British forces employed codes and ciphers to disguise their communications, and took precautionary measures to ensure that crucial messages were not intercepted by the enemy.

Both armies employed replacement codes, where pre-set letters or words replaced other letters or words in communications. This required intense memorization of static codes, or the use of codebooks, which had a high risk of being stolen by rival spies. The codes used in the American Revolution were simple and easy to decipher, permitting both armies to read intercepts with relative ease. In 1777, the Americans unveiled a new mathematical code that remained unbroken throughout the war, but the complexity of the code precluded its daily use and limited its effectiveness to overseas diplomatic dispatches that did not have to be deciphered in a timely manner.

In lieu of complex codes, American cryptologists developed and used secret writing techniques. Disappearing inks are an ancient espionage trick, but during the Revolution, American scientists developed several inks that needed a series of reagents to reveal the hidden message. Some of these inks were waterproof and held up for months in difficult conditions, a necessity for warfare across wild and vast terrain. To further disguise messages, agents were instructed to write their communications between the lines of common publications, such as pamphlets and almanacs.

Intelligence operations abroad and at sea required further technological advances in espionage tradecraft. With the British blockade, American agents had to be ready to conceal or destroy intelligence information that they carried. To preserve and conceal information, agents developed small, silver containers in which information could be hidden. The container could then be thrown into the fire and melted or be swallowed by the agent, permitting information to possibly remain intact and undetected.

After the end of the Revolution, and the establishment of an independent United States government, most military and espionage institutions were dissolved. Until the outbreak of World War I in 1914, American intelligence agencies and services were exclusively wartime organizations, rapidly assembled in times of conflict, and dissolved in times of peace. Though intelligence operations certainly aided the victory of American forces over the larger and better-armed British military, peacetime intelligence remained scattered, and largely focused on political and diplomatic espionage operations.

#### ■ FURTHER READING:

##### BOOKS:

- Finn, Elizabeth. *Pox Americana*. New Haven, CT: Yale University Press, 2000.
- Mahoney, Harry Thayer, and Marjorie Locke. *Gallantry in Action: A Biographic Dictionary of Espionage in the American Revolutionary War*. Lanham, MD: University Press of America, 1999.

##### ELECTRONIC:

- Central Intelligence Agency. "Intelligence in the War of Independence." <<http://www.odci.gov/cia/publications/warindep/frames.html>> (May 19, 2003).

#### SEE ALSO

*War of 1812*

## RF Detection

Among the most potentially damaging weapons of electromagnetic warfare are RF, or radio frequency systems. Also known as directed-energy weapons, these use electromagnetic energy on specific frequencies to disable electronic systems. There exist means to protect against directed-energy weapons; aside from "hardening" computer systems, protection is possible through the employment of electronic RF detection equipment, which operates on a principle similar to that of radar.

In the modern world of sophisticated, computerized fighter jets, the missile systems of one fighter aircraft can only "lock on" and fire on an enemy craft if the enemy has his radar systems activated. The same electronic radio-frequency system that allows a plane to navigate also makes it capable of being tracked electronically across the sky. Similarly, that which makes RF weaponry so potentially threatening—the fact that they can disable flight systems by interfering with vital frequencies on the electromagnetic spectrum—also makes them detectable.

Given the fact that Soviet and Russian technicians have reportedly developed RF weaponry, it is assumed that technicians working for the United States Department of Defense have created RF detection equipment at least as sophisticated. At a much lower end are civilian and consumer versions of computerized RF detection equipment, retailing for a few hundred or thousand dollars. A January 2003 article in the *Wall Street Journal* described a pocket wireless system called Spotme that could read electronic badges on guests at a party and provide the user with other guest's names, photographs, and contact information. For security purposes, there are RF detection consoles that operate across a wide frequency spectrum to search out and identify potentially harmful RF sources.

#### ■ FURTHER READING:

##### PERIODICALS:

- Fund, John. "In the Fray: People Spotters—European Gizmo Tells Who's Who." *Wall Street Journal*. (January 23, 2003): D8.
- Torregrosa-Penalva, German, et al. "Microwave Temperature Compensated Detector Design for Wide Dynamic Range Applications." *Microwave Journal* 44, no. 5 (May 2001): 336–346.

#### SEE ALSO

*Electronic Warfare*



**RADAR**  
Radio Frequency (RF) Weapons

## Ricin

■ JULI BERWALD

Ricin is a highly toxic protein that is derived from the bean of the castor plant (*Ricinus communis*). The toxin causes cell death by inactivating ribosomes, which are responsible for protein synthesis. Ricin can be produced in liquid, crystal or powdered forms, and it can be inhaled, ingested, or injected. It causes fever, cough, weakness, abdominal pain, vomiting, diarrhea, dehydration, and death. There is no cure for Ricin poisoning, and medical treatment is simply supportive.

**Chemical structure and pathological pathway.** Ricin is a protein composed of two hemagglutinins and two toxins (RCL III and RCL IV). The toxins are made up of an A polypeptide chain and a B polypeptide chain, which are joined by a disulfide bond. The general molecular structure of Ricin is similar to other biologically produced toxins, such as botulinum, cholera, diphtheria, and tetanus.

The B portion of Ricin binds to glycoproteins and glycolipids that terminate with galactose on the exterior of cell membranes. Ricin is then transported inside the cell by endocytosis. Once inside the cytosol of the cell, the A portion of the molecule binds to the 60S ribosome, stopping protein synthesis. A single molecule of Ricin can kill a cell.

**Ricin poisoning.** Ricin poisoning can occur by dermal (skin) exposure, aerosol inhalation, ingestion, or injections, and the symptoms vary depending on the route of exposure. If Ricin comes in contact with the skin, it is unlikely to be fatal, unless combined with a solvent such as DMSO. Aerosol inhalation of Ricin can cause symptoms within four to eight hours. Fever, chest tightness, cough, nausea, and joint pain may occur. Ricin can cause cell death in the respiratory system and eventual respiratory failure. If Ricin is ingested, it can cause severe lesions in the digestive system within two hours of exposure. It may cause abdominal pain, nausea, vomiting, and bloody diarrhea. Eventual complications include cell death in the liver, kidney, adrenal glands, and central nervous system. Injection of Ricin causes local cell death in muscles, tissue, and lymph nodes. Ricin poisoning causes death generally within three to five days. If Ricin exposure does not cause death within five days, the victim will probably survive.

There is no cure for Ricin poisoning, although a vaccine is currently under development. Treatment for dermal exposure includes decontamination using soap and water or a hypochlorite (bleach) solution, which deactivates Ricin. In case of aerosol inhalation, treatment is the administration of oxygen, intubation, and ventilation. Ingestion of Ricin is treated with activated charcoal.

**Ricin production and use as a biological weapon.** Ricin comes from castor beans, which produce castor oil, a component of brake fluid and hydraulic fluid. One million tons of castor beans are processed each year and the resulting waste mash contains 5–10% Ricin. The 66,000 Dalton protein can be purified from the mash using chromatography. Once purified, Ricin is a very stable molecule that is able to withstand changes in environmental conditions.

Ricin is considered moderately threatening as a biological warfare agent. Although it is environmentally stable, relatively easy to obtain, highly toxic, and has no vaccine, it is not communicable like other biological agents such as anthrax and smallpox. Ricin is most often considered a threat as a food or water contaminant. A large amount would be required to cover a significant area.

The most famous case involving Ricin is the assassination of the Bulgarian dissident Georgi Markov. In 1978, Markov was working in London as a British Broadcasting Company (BBC) correspondent. As he was walking across Waterloo Bridge, a man jabbed the tip of an umbrella into Markov's right thigh, murmured an apology, and slipped away into the crowd. Markov died four days later. After the collapse of the Soviet Union, the new Bulgarian government admitted that their Secret Service had been responsible for the murder. The KGB produced the murder weapon: an umbrella modified to inject a 1.7 mm platinum pellet filled with Ricin into Markov's leg.

Incidents involving Ricin have occurred in the United States. Four men were convicted of plotting to kill a United States marshal with Ricin in Minnesota in 1991. They were all members of an extremist antigovernment group called the Patriots Council. In 1995, Canadian officials stopped Thomas Lavey at the border with Alaska with a bag of Ricin. He was also in possession of guns, ammunition, manuals for making biological and chemical weapons, and neo-Nazi literature.

Ricin has been loosely linked to the al-Qaeda terrorism network. In January 2002, police in London were advised that a group of men were manufacturing Ricin in their apartment. Although only a small amount of Ricin was found, castor beans as well as equipment for crushing and extracting Ricin from the beans were discovered. Seven men of North African background were arrested in the incident, and security experts speculate that they had links to al-Qaeda. There also are reports that Ricin was found in caves abandoned by the Taliban in Afghanistan.

## ■ FURTHER READING:

### BOOKS:

Haugen, David M., ed. *Biological and Chemical Weapons*. San Diego: Greenhaven Press, Inc., 2001.

Sifton, David W., ed. *PDR Guide to Biological and Chemical Warfare Response*. Montvale, NJ: Thompson/Physician's Desk Reference, 2002.

Wise, David. *Cassidy's Run: The Secret Spy War over Nerve Gas*. New York: Random House, Inc., 2000.

### ELECTRONIC:

Animal Science at Cornell University. "Ricin Toxin From Castor Bean Plant." <<http://www.ansi.cornell.edu/plants/toxicagents/Ricin/Ricin.htm>> (February 5, 2003).

BBC News UK "Seventh Arrest in Ricin Case." <<http://news.bbc.co.uk/1/hi/uk/2637515.stm>> (February 5, 2003).

Medical NBC Online. "Ricin." <<http://www.nbc-med.org/SiteContent/RedRef/OnlineRef/FieldManuals/medman/Ricin.htm>> (February 5, 2003).

Mirarchi, Ferdinando L., eMedicine. "Ricin." <<http://www.emedicine.com/emerg/topic889.htm>> (February 5, 2003).

### SEE ALSO

*Biological Warfare*  
*Bioterrorism*  
*Toxins*

## Robotic Vehicles

### ■ JUDSON KNIGHT

From the late 1980s onward, robotic vehicles have become an increasingly important component of security operations and related activities. They can be used to gather information in areas where a human could not safely go and undertake tasks a human could not safely perform. Robotic vehicles can be used, for instance, in underwater minesweeping, and in sites contaminated by nuclear, biological, or chemical materials. The use of robotic vehicles on scientific expeditions to such inhospitable locales as the polar ice cap and the surface of Mars portends a variety of applications for intelligence gathering. Robotic technology also has uses in energy harvesting, or the gathering of energy from ambient sources such as sunlight, wind, or barometric fluctuations.

### Robotic Operation

A 1994 article in *The Industrial Robot* identified five parameters or "subtasks" of robotic operation: localization, motion control, mapping, path planning, and communication with the operating station. The subtask of localization is a matter highly analogous to human movement. If a person does not know his or her location, that person cannot know where he or she is going; in order to stay on

the right path, it is necessary to receive continual data regarding the environment. For the human mind, these skills are largely automatic—one does not have to think about walking around an obstacle, for instance—but for the robot, course correction must be built into the overall operating system.

Closely related to the problem of localization is that of motion control. Some robots operate on set paths analogous to a railroad track, but as technology has progressed, scientists have developed means that will allow robotic vehicles to operate in a less modified environment, using navigational markers. These markers are reflective targets that serve as beacons, allowing the robotic vehicle to correct its course when it strays from a desired path. Efforts to make these vehicles capable of operating in a completely unrestricted environment are ongoing.

Also closely related to localization is the issue of mapping the environment—a function that, once again, is automatic for humans. Robots use visual, ultrasonic, and touch sensors. More sophisticated machines made for operating in an outdoor locale have means of navigating by visual methods using focus-enhancing technology.

Robotic scientists are using ever more sophisticated means of navigation. Among these is the use of a camera to provide data allowing the home station to implement course correction measures. The Global Positioning System, or GPS, also offers a method of aiding navigation in large, open environments. Still more complex are various techniques applying teleoperation through virtual-reality systems.

**Path planning and communication.** Path planning involves addressing the problem of minimizing the output of time or energy required to reach a certain goal. In spatial terms, path planning involves helping the robot to find the shortest possible distance between two points. Temporal or time-based path planning may be more challenging in view of unpredictable inputs from the environment.

Finally, there is the matter of communication with the home station, a problem encountered by humans in tasks ranging from intelligence gathering to space travel. In addition to receiving information on changing courses or tasks, robots undertaking sophisticated activities may need to send back video data or other forms of intelligence.

### Uses for Robotic Vehicles

The applications, and potential applications, of robotic vehicles are myriad. Within the realm of industry, they can be used for everything from moving containers in ports (an application demonstrated in 1994) to clearing snow off of airport runways. On a consumer level, robotic technology can be employed in wheelchairs and in cleaning homes or offices.

In the realm of scientific study, robotic vehicles provide a means of conducting research in environments that



A British Army robot inspects a suspect vehicle for explosives outside the Europa Hotel in Belfast, Northern Ireland. AP/WIDE WORLD PHOTOS.

are either presently or forever inaccessible to humans. The use of a robotic vehicle to collect data during the 1997 National Aeronautics and Space Administration (NASA) Mars Pathfinder Expedition gained widespread attention, but scientists also use robots much closer to home. Small, submarine-like robots known as autonomous underwater vehicles (AUVs) have in some cases taken the place of acoustic remote-sensing technology to map seabed topography. They also offer promise in areas impenetrable to more traditional methods—for instance, for mapping hydrothermal vents beneath the Arctic Ocean.

**Security and related activities.** Applications for robotic technology in security and related functions are fast emerging. At the simplest level, a robotic vehicle “walking a beat” could be used to patrol a parking garage by providing real-time video data to a facility security station. The U.S. Navy in the 1980s began using AUVs to conduct minesweeping operations in the Persian Gulf. In 1996, scientists at Lawrence Livermore National Laboratory created a prototype for a robotic vehicle that could be outfitted for a variety of tasks, including not only mine detection and clearance, but also intelligence-gathering.

In 2000, *Design News* reported that technicians at Sandia National Laboratory were in the process of developing a highly sophisticated machine called a MARV, or

miniature autonomous robotic vehicle. Very small—a cubic inch (16.4 cc) in size—the MARV is designed to “rove in packs” for purposes such as surveying a contaminated area, sweeping for and disabling mines, or locating biological weapons. Engineers at Sandia have addressed the problem of course correction through genetic algorithm-based software, a fascinating innovation intended to mimic the functions of a human brain.

**Energy harvesting.** An area of research in which robotic technology plays a dual role, both as a tool and as a potential beneficiary, is energy harvesting. The latter is the gathering of energy from ambient sources, including sunlight, wind, wave action, water currents, geothermal components such as volcanoes, chemical and thermal gradients, barometric fluctuations, electromagnetic radiation, and human and other biological systems. The aim of energy-harvesting efforts using robotic technology and other means is to increase the efficiency of power delivery by a factor of 10 with respect to conventional systems.

The U.S. Defense Advanced Research Projects Agency (DARPA) has expressed an interest in developing robotic technology for the purposes of energy harvesting, as well as using energy-harvesting methods to supply power to robotic vehicles. In 1997, DARPA allocated \$25 million toward energy-harvesting projects, among which was a

robotic “boot” (functional by 2001) that harvests energy from walking.

In 2002, engineers at Pennsylvania State University introduced an optimized energy-harvesting circuit capable of improving retrieval systems from vibration—including that of machine operation and human motion—by a factor of four. Among the applications for this energy-harvesting technology, researchers noted, were robotic control and guidance systems to be used in manufacturing and other activities.

#### ■ FURTHER READING:

##### PERIODICALS:

- “Circuit Transfers Four Times More Power out of Vibration.” *Resource* 9, no. 11 (November 2002): 6.
- “Designed for Danger.” *Design News* 55, no. 2 (January 17, 2000): 28.
- “EDM on Mission to Mars.” *Manufacturing Engineering* 119, no. 4 (October 1997): 116.
- Evers, Stacey. “DARPA to Reap Benefits of ‘Energy Harvesting’.” *Jane’s Defence Weekly*. (November 26, 1997): 8.
- Jarvis, Ray. “Robot Navigation.” *The Industrial Robot* 21, no. 2 (1994): 3.
- “Novel Design of Countermine Robot.” *Jane’s International Defense Review* (February 1, 1996): 20.
- “Robo P.I.” *American Scientist* 90, no. 1 (January/February 2002): 28–29.
- Treherne, Jan. “Robotic Roads—Pathways to the Future.” *The Industrial Robot* 21, no. 5 (1994): 3.

##### ELECTRONIC:

Energy Harvesting. Defense Advanced Research Projects Agency. <<http://www.darpa.mil/dso/trans/energy/>> (April 15, 2003).

##### SEE ALSO

*DARPA (Defense Advanced Research Projects Agency)*  
*GPS*  
*NASA (National Air and Space Administration)*  
*Unmanned Aerial Vehicles (UAVs)*

---

## Romania, Intelligence and Security

---

A former Soviet bloc country, Romania is struggling to rebuild its national government and economy following the collapse of Soviet communism. Romania further struggled to free its government of authoritarian influences. In 1989, nationalist forces arrested, tried, and executed dictator Nicolae Ceausescu, beginning the arduous process

of democratizing the Romanian government. During Ceausescu’s rule, Romanian intelligence and security forces conducted a brutal campaign to crush political dissent. The government now endeavors to distance Romania’s new intelligence and security community with the legacy of its predecessors. However, lingering public suspicion of government agencies and police forces has proved difficult to overcome.

The Office of the President oversees Romania’s primary domestic intelligence and security services. The Romanian Intelligence Service (SRI) is the nation’s main internal intelligence agency. The agency is responsible for assessing threats to national security, conducting surveillance on behalf of the military and government, and protecting national economic interests. Though the agency has been reformed several times since 1990, public suspicion about the secretive nature of domestic intelligence policy persists. Parliamentary restrictions place on the SRI include the necessity to obtain warrants for most surveillance operations, and a permanent ban on using intelligence service equipment and personnel for political reasons. To help assuage public concerns, the SRI is one of two Romanian intelligence agencies whose organization and operation is subject to parliamentary review.

The SRI works closely with the Guard and Protection Service (SSP), a national law enforcement agency. The SSP is charged with the protection of government officials and foreign diplomats. In cooperation with the Romanian Intelligence Service, the SSP functions as a special action unit for anti-terrorism operations.

The Ministry of the Interior controls Romania’s civilian intelligence community. Known as the Securitate, the Department of State Security was the communist-era intelligence agency that worked with the secret police forces to conduct domestic espionage. Post-Cold War democratic reforms dissolved the Securitate and created new agencies, none of which are authorized to conduct espionage activities on Romanian citizens. The Interior Ministry Intelligence Directorate (UM 0251) now directs civilian intelligence and security service operations. The agency is charged with protecting national security. The Gendarmerie, the national police force, aids Romanian intelligence services to insure public safety.

Foreign intelligence is coordinated through the Ministry of Foreign Affairs (MAE). The Ministry employs its own intelligence force, the Foreign Intelligence Service (SIE). The SIE analyzes external threats to Romanian interests.

The Romanian military operates its own intelligence forces in specially trained units. The Ministry of National Defense coordinates some military intelligence operations through various operational branches. The Special Telecommunications Services specializes in communications security. The Counter-Intelligence Directorate oversees military, and sometimes civilian, counterintelligence operations. The Intelligence Directorate of the Army also operates within the Ministry of National Defense,

coordinating operations to assess and preserve national security using military intelligence resources.

#### SEE ALSO

*Cold War (1972–1989): The Collapse of the Soviet Union European Union*

## Room 40

■ ADRIENNE WILMOTH LERNER

Advances in communications technology such as the telephone and trans-Atlantic telegraph prompted the development of increasingly sophisticated cipher systems and codes. The telegraph facilitated communication between command and remote forces, but the lines were vulnerable to tapping, the interception of message traffic, on the wires. As codes became more mathematical and complicated, intelligence services enlisted professional cryptologists, or code breakers, and language translators.

At the outbreak of World War I in 1914, British intelligence began intercepting wire transmissions sent by the German military and government. The German cipher was unknown, so British intelligence quickly established a cryptography department to begin the task of breaking enemy code. The department, under the direction of intelligence officer Reginald “Blinker” Hall and code expert Alfred Ewing, was located in Room 40 of the Admiralty Building. The cryptology department housed in Room 40 was only a small branch of Britain’s large intelligence system. However, after remarkable successes achieved by the team, Room 40 became a catch-all nickname for British military intelligence during the war.

While the cipher systems themselves were becoming more complex in the early twentieth century, the technology to decode them had not advanced at the same pace. Codes were still worked out by hand in long sequences to look for mathematical permutations and deviations from known ciphers that formed essential code patterns. The best means of breaking code was to capture an enemy codebook. Beginning in 1914, an extraordinary string of events led to the capture of not one, but three different German code books, allowing Room 40 to intercept, decode, and translate most German military and diplomatic transmissions.

Early in the war, a box recovered from a sunken German submarine yielded a copy of the German Foreign Office codebook. British intelligence was thus able to monitor diplomatic correspondence between the German government and its territories and embassies. Similarly fortuitous for Room 40, later that year a German cruiser was sunk by the Russian Navy. When the Russian fleet rescued surviving German sailors from the downed ship, one officer was found to have a copy of the German Naval

codebook. The codebook was sent to British intelligence, and Room 40 was able to decipher wire traffic from German fleet commanders and ships. As most ships in the German fleet reported their positions daily, British intelligence learned individual ship identification codes and tracked the position of most German warships and submarines by the end of 1915.

While the two recovered codebooks let British military intelligence decipher nearly a quarter of German military transmissions, the capture of a third codebook in 1915 gave Room 40 the mathematical key to German cipher system. Wilhelm Wassmuss, the German consul in Persia, hastily fled his office to escape encroaching British forces, leaving behind his copy of the German diplomatic codebook. Room 40 cryptographers discovered that the first two codebooks recovered were standard permutations of the third code. Thus, several German codes were based on a single cipher system and, by applying systematic variations, British cryptographers were able to break the remaining codes.

In 1917, Room 40 had its greatest success. The United States, while holding Allied sympathies and aiding the transportation of ammunition across the Atlantic Ocean, held fast to a policy of non-intervention in the war. Increased German submarine warfare, the sinking of U.S. and Allied merchant and passenger ships, and the work of German saboteurs in the Black Tom explosion fostered a shift in American attitudes toward entering the war. On the morning of January 17, 1917, British military intelligence intercepted secret communication from German Foreign Minister Arthur Zimmerman to the German ambassador in Washington, D.C. The message took cryptographers nearly a month to decode in whole, but the importance of the telegram was realized almost immediately. The Zimmerman Telegram, as it became known, revealed German plans to begin unrestricted submarine warfare in the Atlantic. Knowing that this could bring America into the war, Germany planned to make alliances with Mexico and Japan to keep the U.S. occupied on its own ground instead of in Europe. The telegram not only spoke of driving England to surrender, but also promised Mexico the return of its former territories in Texas, New Mexico, and Arizona. British intelligence shared the contents of the memo with the American government, thwarting the German plan. Declaring war on Germany shortly after, America entered the war in Europe.

In 1918, Room 40 intercepted transmissions that revealed that a sizable group of German sailors had mutinied. News of a German surrender soon followed. The triumphs of Room 40 during the course of World War I convinced the British Admiralty that cryptography was a necessary tool of modern warfare. By the advent of World War II, however, the field of cryptography significantly changed with the introduction of cipher machines, teleprinters, and radio.

#### SEE ALSO

*Black Tom Explosion*

World War I  
World War I: Loss of the German Codebook

## Rosenberg (Ethel and Julius) Espionage Case

■ ADRIENNE WILMOTH LERNER

Julius and Ethel Rosenberg were a couple accused in 1950 by the United States government of operating a Soviet spy network and giving the Soviet Union plans for the atomic bomb. During a time of tense scrutiny over alleged communist infiltration of the American government, the trial of the Rosenbergs became the center of a political storm over communist influence in America. Their trial was one of the most controversial of the twentieth century, ending with their execution.

Julius Rosenberg was a committed communist who had graduated from the City College of New York in 1939 with a degree in electrical engineering. He married Ethel Greenglass in the summer of that year. She was a headstrong woman, active in organizing labor groups. Julius had opened a mechanic shop with his brother-in-law, but the business soon began to fail, largely due to lack of attention by Julius, who invested his time spying for the Soviets. He began by stealing manuals for radar tubes and proximity fuses, and by the late 1940s, had two apartments set up as microfilm laboratories.

The arrest of the Rosenbergs was set in motion when the FBI arrested Klaus Fuchs, a British scientist who gave atomic secrets to the Soviets while working on the Manhattan Project. Fuchs's arrest and confession led to the arrest of Harry Gold, a courier for Soviet spies. Gold in turn led investigators to David Greenglass, a minor spy who confessed quickly. Greenglass then accused his sister Ethel and brother-in-law Julius of controlling his activities.

Julius immediately realized the implications of Harry Gold's arrest and began to make arrangements to get out of the country, but the FBI moved swiftly. Julius Rosenberg was arrested in July 1950.

Ethel Rosenberg was later arrested in August. Although Federal investigators had little evidence against her, they hoped to use the threat of prosecuting her as a lever to persuade Julius to confess. The plan failed, and the couple was charged with conspiracy to commit espionage. Their trial began on March 6, 1951.

From the beginning, the trial attracted national attention. The prosecution decided to keep the scope of the trial as narrow as possible, with establishing the Rosenbergs' guilt the main target, and exposing their spy ring a lesser concern. Nonetheless, the trial was punctuated by numerous arrests of spies associated with the Rosenbergs, some appearing in court to testify against them.



Ethel Rosenberg and her husband Julius are separated by a wire screen as they ride to separate jails in New York City in 1951 after their conviction for delivering secrets, including vital atomic bomb data, to the Soviet Union. AP/WIDE WORLD PHOTOS.

The defense tried to downplay the importance of the information the prosecution claimed the Rosenbergs had stolen, but then turned around and requested that all spectators and reporters be barred from the courtroom when the information was discussed.

The Rosenbergs accused David Greenglass of turning on them because of their failed business, but these efforts only elicited sympathy for a man who had been forced to turn in a family member. Greenglass damaged the Rosenbergs by testifying that Julius had arranged for him to give Harry Gold the design of the atomic bomb used on Nagasaki (which differed considerably from the Hiroshima bomb). When Gold himself testified, he named Anatoli Yakovlev as his contact. This directly tied the Rosenbergs to a known Soviet agent. Julius and Ethel Rosenberg were found guilty on several accounts of espionage and conspiracy. They were sentenced to execution, a sentence usually reserved for cases of treason.

After months in prison, the Rosenbergs still maintained their innocence and began to write poignant letters, which were widely published, protesting their treatment. The case was followed closely in Europe, where many felt the Rosenbergs were being persecuted because they were Jewish (though Judge Kaufman was also Jewish). A movement began to protest the "injustice" of the Rosenberg

trial. Passions both for and against the Rosenbergs grew so great that they even threatened Franco-American relations, as the French were particularly harsh in their condemnation of the trial as a sham.

In the months between the sentencing and execution, criticism of the trial grew more strident, and major demonstrations were held. Nobel-prize winner Jean-Paul Sartre called the case “a legal lynching which smears with blood a whole nation.” In spite of attempts at appeal and a temporary stay issued by Supreme Court Justice William O. Douglas, Julius and Ethel Rosenberg were executed on June 19, 1953, both refusing to confess.

Years after the event, the case continues to stir debate. Although the Rosenbergs were communists and engaged in espionage, they did not spy for an enemy of the United States, as the sentence might indicate, but rather for its wartime ally. Recent studies of the couple’s activities show that the evidence against them was overwhelming. The declassification and release of Venona transcripts (a secret, decades-long, general surveillance operation) further implicated the Rosenbergs. Regardless of the evidence, the political and social upheaval surrounding the trial, and its ultimate outcome, can only be understood through the lens of heightened Cold War tensions and anti-Communist hysteria.

#### ■ FURTHER READING:

##### BOOKS:

Nash, Jay Robert. *Spies: A Narrative Encyclopedia of Dirty Deeds and Double Dealing from Biblical Times to Today*. M.Evans, 1997.

##### SEE ALSO

*Cold War (1945–1950), The Start of the Atomic Age*  
 KGB (Komitet Gosudarstvennoi Bezopasnosti, *USSR Committee of State Security*)  
*McCarthyism*

---

## Russia, Intelligence and Security

---

The Russian Empire dominated Eastern Europe and Western Asia from the Middle Ages through the nineteenth century. However, the devastation caused by World War I plunged the nation into revolution in 1917, leading to an overthrow of the Czarist regime and the birth of communism. The communist government created a large intelligence community, with secret police forces, to conduct political espionage on ordinary citizens. The era was marred by political show trials and the harsh imprisonment of

political dissidents. Before the outbreak of World War II, the oppressive regime of Joseph Stalin centralized the nation’s agricultural and industrial systems. Despite the rapid industrialization and growth of the national military infrastructure, the ensuing economic turmoil, brutal political oppression, and famine cost millions of lives.

Russia entered World War II as a member of the Allied forces. Their participation in the war effort was key to the Allied defeat of Germany in 1945. Although Russia was a strategic wartime ally, relations between Russia and the West, particularly the United States, quickly soured in the first post-war months. The diplomatic, economic, and military standoff between the United States and Russia intensified into the decades-long Cold War. The nations engaged in an intelligence war in lieu of military conflict, and the antagonism between the two states redefined their national intelligence services and modern espionage tradecraft.

Hard-line communism fell out of favor in Russia as the national economy plummeted in the 1980s. A period of détente between Russia and the West allowed General Secretary Mikhail Gorbachev to implement a series of political and economic reforms, known as Glasnost and Perestroika. Reforms were also made to the national intelligence super-agency, the KGB. Though the leader sought to modernize the face of communism, the reform programs sped the regime’s eventual downfall. The Soviet Union splintered in 1991. The largest former province, and the heart of the old Russian Empire, became the Russian Federation. Since the creation of the democratic republic, the nation has struggled to reform its national political system and its intelligence community.

Since the breakup of the Soviet Union, Russia’s intelligence and security agencies have been administered, and influenced, by the Office of the President of the Russian Federation. The executive branch governs the intelligence community via the Russian National Security Council, and the Defense council. The two boards act as a liaison between the government and the intelligence services, briefing the executive and legislature when national security threats arise. Since the Russian intelligence community is now more departmentalized than it was under Soviet control, the two councils help to centralize the dissemination of intelligence information and the formation of intelligence policy.

The *Federal’naya Sluzhba Bezopasnosti*, Federal Security Service (FSB), a successor agency of the Soviet KGB and Russian Federal Counterintelligence Service (FSK), is Russia’s counterintelligence agency. FSB operations focus on domestic counterespionage and internal security. Headquartered in Lubyanka, the agency employs over 75,000 people. Since the creation of the agency, the Russian government has placed increasing limitation on FSB operations to guard against abuse of intelligence community resources. Russian law now severely restricts FSB surveillance operations conducted against ordinary citizens, and new constitutional reforms seek to prohibit the use of FSB forces for political espionage.

In response to the growth of organized crime after the dissolution of the Soviet Union, the Russian intelligence community established the Main Administration for Organized Crime (RUOP). The agency uses human and remote intelligence to infiltrate and investigate crime syndicates operating within Russia's borders. Despite ongoing efforts of the agency, organized crime has increased in Russia.

Russian intelligence operates special assignment bureaus in Kaliningrad and Chechnya. The Russian military's involvement in the region, and endemic conflict between nationalist and Russian factions, prompted the intelligence community to form task forces devoted to counterterrorism and counterintelligence. These operational units are usually a mix of civilian and military intelligence personnel and report to a variety of agencies, including the FSB and the Russian Security Council.

Though Russia has attempted to distance its new intelligence community from the legacy of the Soviet KGB and internal secret police forces, many of its new national intelligence agencies are indeed successor organizations of specialized departments within the former KGB. The Foreign Intelligence Service (SVR) was one of the first operational departments of the KGB to emerge as its own intelligence entity. The SVR now oversees most of Russia's foreign intelligence operations, including collection and analysis of data. The main intelligence objectives of the SVR are to collect information on rival military and economic powers. In 1995, the head of the SVR claimed that expansion of the North Atlantic Treaty Organization (NATO) was the largest threat to Russian sovereignty and regional influence. In response to the perceived threat, the SVR conducts routine foreign intelligence surveillance of the former Soviet republics.

In the late 1990s, the focus of SVR operations shifted from military-related foreign intelligence to industrial, scientific, and technological espionage. Several divisions within the SVR use extensive human and remote intelligence networks to collect information on rival economies. Russian intelligence operated its own intelligence gathering missions in Asia and the West, but also devoted considerable resources to counterintelligence in a bid to protect Russian industry. The rise of the European Union (EU) prompted Russia to take a more strident political stance on international trade laws. However, in 2000, the nation refused to join a UN Security Council-led effort to limit economic espionage and prosecute industrial spies.

Russia's misleadingly named Main intelligence Agency (GRU) is the nation's primary intelligence information clearinghouse and analysis bureau. Though the agency does conduct intelligence gathering missions, its primary duty is to coordinate inter-agency information operations and process intelligence materials.

Russia garnered international criticism for its lack of security and protective intelligence measures against the proliferation of weapons from the former Soviet Union. Russia now devotes considerable intelligence resources

to international non-proliferation efforts. However, national intelligence and security services have had little efficacy against criminal organizations and individuals selling arms and weaponry to terrorist groups and rogue states.

Russian foreign policy continues to evolve. Despite hostilities toward EU and NATO expansion, the Russian government has cooperated with European and United Nations anti-terrorism efforts. In 2003, Russia, with the diplomatic cooperation of France and Germany, moved to block UN-sanctioned military action against Iraq.

#### ■ FURTHER READING:

##### ELECTRONIC:

CIA World Factbook. "Russia" <<http://www.cia.gov/cia/publications/factbook/geos/rs.html>>(May 5, 2003).

##### SEE ALSO

*Cold War (1945–1950), The Start of the Atomic Age*

*Cold War (1950–1972)*

*Cold War (1972–1989): The Collapse of the Soviet Union KGB (Komitet Gosudarstvennoi Bezopasnosti, USSR Committee of State Security)*

---

## Russian Nuclear Materials, Security Issues

---

■ MICHAEL J. O'NEAL

The breakup of the former Soviet Union in 1991 raised fears about the disposition and security of that nation's nuclear materials, including its strategic and tactical nuclear weapons. Of more immediate concern is the security of Soviet stores of plutonium and enriched uranium, which could be used to make either nuclear weapons or "radiological dispersal devices" (RDDs), or "dirty bombs"—conventional explosives that would spew radioactive debris packed around them over a wide area. Since 1991, the United States has provided financial and technical assistance to help Russia and other former Soviet states secure these materials.

**Background.** During the cold war, the Soviet Union, like the United States, amassed an imposing stockpile of nuclear weapons. Western estimates were that by 1991 the Soviets had in excess of 27,000 nuclear weapons—at least 11,000 strategic weapons on land-based intercontinental ballistic missiles (ICBMs) and at least 15,000 warheads for tactical weapons such as artillery shells and cruise missiles. Later information suggested that the total might



have been as high as 45,000 warheads. Additionally, the Soviets had as much as 1,200 metric tons of weapons-grade uranium and 160 metric tons of plutonium, enough to triple their stockpile of nuclear weapons. Eighty percent of the strategic weapons were deployed at bases in Russia, but the remainder were deployed in the Soviet republics of Ukraine, Belarus, and Kazakhstan. Tactical nuclear weapons were deployed closer to potential theaters of operation, including Eastern Europe and the former Baltic republics. Still others were deployed in Armenia, Azerbaijan, Belarus, Ukraine, Kazakhstan, Georgia, and the Central Asian states (Kirghizia, Tajikistan, Turkmenistan, Uzbekistan).

While these nuclear materials were under the command and control of Soviet authorities in Moscow, the chief threat they posed to the West was strategic: They could be used against the West in a nuclear exchange. Regardless, in contrast to the modern situation, Soviet authorities maintained account of these materials and security around nuclear facilities was tight. Weapons could be fired only through a central command authority. Although an enemy to the West, the Soviet regime was at least a politically stable state that could be anticipated act rationally in its own self-interest, and which was unlikely to allow the use of nuclear materials for terrorist purposes. Essentially, the threat that nuclear materials posed to the West was predictable, manageable, and able to be reduced through negotiation and arms-control treaties.

The status quo began to change in the 1980s. The Soviets were finding it increasingly difficult to maintain control over an enormous empire that stretched from the German border to Asia. They also faced increasingly restive ethnic and national populations demanding self-determination. Under these pressures, the Soviet Union began to disintegrate and finally collapsed in late 1991. By then, the Soviets had retrieved their nuclear materials from Eastern Europe and the Baltics, as well as from submarines, but many remained closer to home, primarily in Georgia, Ukraine, Belarus, and Kazakhstan. Eventually, and after much diplomatic wrangling, these new nations agreed to the Nuclear Non-Proliferation Treaty and either destroyed the missiles and warheads on their soil or returned them to Russia, though stockpiles of plutonium and weapons-grade uranium remained behind. Security surrounding these materials, and at nuclear power plants, was often lax, raising fears that they could fall into the wrong hands. Within Russia, a poor economy, crime, and corruption raised fears of "loose nukes," or poorly guarded nuclear materials that could be stolen or sold to rogue states such as Iraq or Libya or to terrorist organizations, primarily al-Qaeda. The United States estimates that only about 40 percent of Russia's nuclear storage sites are up to U.S. security standards.

**The U.S. response.** Recognizing the need for the United States to provide assistance, Senators Sam Nunn of Georgia and Richard Lugar of Indiana sponsored legislation that allocated funds to help Russia and other former

Soviet states either dismantle or secure nuclear materials. Congress agreed, and in 1991–92 it authorized \$800 million for the Nunn-Lugar Cooperative Threat Reduction Program. Each year after that, additional funds were authorized so that by 2001 the United States had provided \$4 billion. These funds have been used by the Department of Defense (DOD), the Department of Energy (DOE), and other U.S. agencies to help the Soviet states destroy nuclear materials, upgrade security, and provide alternative employment for former Soviet nuclear scientists.

Nunn-Lugar funds have helped Russia, for example, deactivate nearly 5,800 nuclear warheads, destroy 439 ballistic missiles, eliminate hundreds of missile launchers and bomber aircraft, and secure nuclear materials by upgrading fencing, motion sensors, storage and transportation facilities, and the like. Originally, the George W. Bush administration had planned to cut funding for the program, but in the wake of the terrorist attacks on September 11, 2001, 2003 budget proposals called for \$800 million for Russia, a 17 percent increase from 2002. Financial help is coming from other sources, too. At a 2002 summit, the industrialized nations pledged an additional \$10 billion over the next ten years to help Russia eliminate or secure its nuclear arsenal, as well as its chemical and biological weapons.

**The threat of "loose nukes."** The true extent of the threat of "loose nukes" is uncertain and may never be known conclusively. Because of poor documentation at Russian nuclear storage sites, for example, materials could disappear, and it is plausible that no one in authority would know their status. Analysts thought that the problem was easing in the mid-1990s, but in the late 1990s and into the new century, instances of black-market smuggling seemed to be on the increase. Since 1993, the International Atomic Energy Agency (IAEA) in Vienna, Austria, a watchdog agency of the United Nations, has reported 411 cases of trafficking in nuclear materials. While 18 cases involved plutonium or weapons-grade uranium, most cases involved low-level medical and industrial radioactive waste, the kind used in dirty bombs. The first documented case of stolen Russian nuclear materials occurred in 1992, when an engineer at a nuclear research facility near Moscow stole three pounds of weapons-grade uranium. Fortunately, the case was resolved in almost comic fashion when the engineer was accidentally swept up in an arrest of a group of his neighbors suspected of theft from their workplace, and the uranium was discovered. Other cases have been more chilling. In 1994, Czech authorities searched a car parked on a street in Prague and discovered 3 kilograms of enriched uranium that came from an engineering institute near Moscow. Since 1999, three similar cases have been reported in Paris and Germany and at the Bulgarian-Romanian border.

An open question concerns the likelihood that an actual weapon could be stolen. The former Soviet states, including Russia, insist that no weapons have been stolen or reported missing, despite numerous efforts on the part

of terrorists and others to get their hands on one. Russian officials say that they have been vigilant in breaking up hundreds of plots to steal and smuggle nuclear materials and weapons, but U.S. officials believe that al-Qaeda and rogue states are always in the market for a nuclear bomb and could eventually succeed in getting one. More frightening is the prospect that poorly paid or unemployed Russian nuclear scientists might be vulnerable to the temptation to sell their know-how to terrorists or rogue states. The Japanese doomsday cult Aum Shinrikyo and the Taliban regime in Afghanistan tried, without success, to recruit Russian nuclear scientists.

Most troublesome is the possibility that so-called suitcase bombs—miniature nuclear devices weighing less than a hundred pounds and small enough to fit into a small container—have gone missing from Russia. These bombs could easily be smuggled into the United States or other countries, where they would cause enormous death and destruction. Indeed, in 1997 a former Russian general made headlines when he claimed that several dozen such Soviet-made bombs dating to the 1970s were unaccounted for. While Russian authorities insist that no such bombs ever existed, many Western analysts remain skeptical. Even if suitcase bombs never existed, the threat remains that small tactical nuclear weapons could be stolen or sold. These weapons pose a high threat for two reasons besides the relative ease with which they could be transported and hidden: one, they may lack safeguards that would prevent unauthorized detonation; and two, they have never been subject to arms-control treaty monitoring and verification, so their locations and the security surrounding them are difficult to assess.

## ■ FURTHER READING:

### BOOKS:

Bunn, Matthew, Oleg Bukharin, and Kenneth N. Luongo. *Renewing the Partnership: Recommendations for Accelerated Action to Secure Nuclear Material in the Former Soviet Union*. Princeton, N.J.: Russian American Nuclear Security Advisory Council, 2000.

Marples, David R., and Marilyn J. Young, eds. *Nuclear Energy and Security in the Former Soviet Union*. Boulder, Colo.: Westview, 1997.

### PERIODICALS:

Daughtry, Emily Ewell, and Fred L. Wehling. "Cooperative Efforts to Secure Fissile Material in the NIS." *Nonproliferation Review* 7, Spring 2000.

### ELECTRONIC:

Council on Foreign Relations. "Loose Nukes," 2003. <[http://www.terrorismanswers.com/weapons/loosenukes\\_print.html](http://www.terrorismanswers.com/weapons/loosenukes_print.html)> (February 28, 2003).

Jasinski, Michael. "Nonproliferation Assistance to Russia and the New Independent States." Center for Nonproliferation Studies for the Nuclear Threat Initiative, August 2002. <[http://www.nti.org/e\\_research/e3\\_4b.html](http://www.nti.org/e_research/e3_4b.html)>. (February 28, 2003).

Wolf, Amy F. "Nuclear Weapons in the Former Soviet Union: Location, Command, and Control." Congressional Research Service Report 91144, November 27, 1996. <<http://www.fas.org/spp/starwars/crs/91-144.htm>> (February 28, 2003).

### SEE ALSO

*Arms Control, United States Bureau Ballistic Missiles*  
*Cold War (1972–1989): The Collapse of the Soviet Union*  
*Department of State, United States*  
*DoD (United States Department of Defense)*  
*DoE (United States Department of Energy)*  
*International Atomic Energy Agency (IAEA)*  
*Nonproliferation and National Security, United States*

*This page intentionally left blank*

# S

## Sabotage

Sabotage is a deliberate act of destruction or work stoppage intended to undermine the activities of a larger entity, whether it is a business, government, or some other organization. The practice of sabotage, which has roots in the labor movements of the late nineteenth and early twentieth centuries, gained military and political application during the world wars and thereafter. It has also been a part of covert operations, often undertaken by agents provocateur.

There were isolated examples in earlier times, but probably the first case of organized—albeit apparently spontaneous—sabotage involved the Luddites of late eighteenth century England. Confronted by nascent industrialization and eager to hold on to their jobs, the Luddites destroyed labor-saving machinery. In 1910, striking French railway workers destroyed wooden railway ties or shoes, known as *sabots*, and from this act the word was coined. Ironically, a concept associated with labor movements was also used against organized labor by factory owners who hired agents provocateurs, infiltrators whose aim was to incite the local union to acts that would attract the attention of police.



Sabotage is suspected in the September 2002 derailment of an express train on its way from Calcutta to New Delhi in the Indian state of Bihar, leaving one car plunged into a river and two others dangling from a bridge. Fifty people died and 180 were injured. AP/WIDE WORLD PHOTOS.

In World War I, the Germans allowed Bolshevik leader V. I. Lenin to enter Russia through their territory, their intention being to sabotage the Russian leadership and pull the country out of the war—a gambit that succeeded. Although the Axis powers attempted to use sabotage against the United States, the most successful act of sabotage in World War II was the British and Norwegian effort to destroy the Germans' supply of heavy water, thus dashing Hitler's plans to build an atomic bomb.

During the postwar era, anticolonial movements in what came to be known as the developing world often used sabotage to remove Western influence. These acts ranged from the passive resistance to British rule by Indians under the leadership of Mohandas K. Gandhi, to the destruction of railway lines by revolutionaries fighting against the Portuguese in Angola and Mozambique. Communist-backed groups often used sabotage, although in Communist countries, any hint of real or imagined sabotage directed against the ruling system met with swift and severe punishment.

#### ■ FURTHER READING:

##### BOOKS:

Bailey, Brian J. *The Luddite Rebellion*. New York: New York University Press, 1998.

Gallagher, Thomas Michael. *Assault in Norway: Sabotaging the Nazi Nuclear Bomb*. New York: Harcourt Brace Jovanovich, 1975.

Julitte, Pierre. *Block 26: Sabotage at Buchenwald*. Garden City, NY: Doubleday, 1971.

Sayers, Michael, and Albert Eugene Kahn. *Sabotage! The Secret War against America*. New York: Harper & Brothers, 1942.

Witcover, Jules. *Sabotage at Black Tom: Imperial Germany's Secret War in America, 1914–1917*. Chapel Hill, NC: Algonquin Books, 1989.

##### SEE ALSO

*Intelligence Agent Soviet Union (USSR), Intelligence and Security*

(although, in fact, civilians have been attacked). Its adherents abroad appear to have largely co-opted the external networks of the GIA, active particularly throughout Europe, Africa, and the Middle East .

**Organization activities.** The GSPC continues to conduct operations aimed at government and military targets, primarily in rural areas. Such operations include false roadblocks and attacks against convoys transporting military, police, or other government personnel. According to press reporting, some GSPC members in Europe maintain contacts with other North African extremists sympathetic to al-Qaeda, a number of whom were implicated in terrorist plots during 2001.

**Estimated organization strength and areas of operation.** Although exact numbers are not known, intelligence analysts estimate that there are probably several hundred to several thousand GIA members operating inside Algeria .

GIA is supported by Algerian expatriates and GSPC members abroad, many residing in Western Europe, who provide financial and logistics support. In addition, the Algerian Government has previously accused Iran and Sudan of support of Algerian extremists.

#### ■ FURTHER READING:

##### ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001, Annual Report: On the Record Briefing. May 21, 2002 <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

##### SEE ALSO

*Terrorism, Philosophical and Ideological Origins Terrorist and Para-State Organizations Terrorist Organization List, United States Terrorist Organizations, Freezing of Assets*

## Salafist Group for Call and Combat (GSPC)

The Salafist Group for Call and Combat (GSPC) splinter faction that began in 1996 has eclipsed the *Groupe Islamique Armé* (GIA or Armed Islamic Group). since approximately 1998, and currently is assessed to be the most effective remaining armed group inside Algeria. In contrast to the GIA, the GSPC has gained popular support through its pledge to avoid civilian attacks inside Algeria

## Salmonella and Salmonella Food Poisoning

#### ■ BRIAN HOYLE

Salmonella is the name of a group, or genus, of bacteria that live in the intestinal tract of warm-blooded animals,

including humans, as well as in cold-blooded animals such as turtles. The name of the microbe comes from its discoverer. In 1885, American veterinary scientist Daniel Salmon isolated the first strain (*Salmonella choleraesuis*) from the intestine of a pig.

Since his discovery, more than 2,300 different types of Salmonella have been discovered. While many of these can be innocuous in their normal intestinal environment, if they infect another area of the body (i.e., a cut) or contaminate food, illness can result.

Salmonella food poisoning, salmonellosis, affects two to four million Americans each year. The number of cases has been increasing in recent years, due in part to the increasing resistance of Salmonella to the antibiotics commonly used to treat the illness. It has been estimated by the Centers for Disease Control and Prevention that the economic cost of Salmonella food poisoning in the U.S. alone is between five and 17 billion dollars annually.

This economic burden, increasing prevalence of Salmonella food-borne illness, and the ease by which disease-causing strains of Salmonella could be acquired and deliberately added to food supplies, have made Salmonella one of the microorganisms that is regarded as being a potential threat to national security.

Salmonella food poisoning results from the growth of the bacterium in food. The rapid increase in the number of bacteria in the intestinal tract overwhelms the defensive capabilities of the host and produces the symptoms of food poisoning. Symptoms include nausea, vomiting, abdominal cramps, diarrhea, fever, and headache. Typically, the symptoms last for a few days.

Prolonged diarrhea can be dangerous. The body loses more fluids and salts than can be replaced, which can threaten the health of various organs and tissues in the body. In severe cases, especially in the young and the elderly, the resulting shock can cause permanent damage. As well, Salmonella can spread from the intestinal tract to the bloodstream, leading to more widespread infections.

The food poisoning caused by Salmonella is one of about ten bacterial causes of food poisoning. Other responsible bacteria include *Staphylococcus aureus*, *Clostridium perfringens*, *Vibrio parahaemolyticus*, and specific strains of *Escherichia coli*.

A number of foods are especially susceptible to contamination. Chicken carcasses and the outer surface of eggs are frequently contaminated with Salmonella present in the poultry feces. However, proper cooking will destroy the bacteria. The bacteria can gain entry to eggs through cracks in the shell. If the egg or meat is prepared at too low a temperature, the bacteria can survive and can multiply during subsequent storage at room temperature, or even at refrigeration temperature. Other targets for contamination include cream-based desserts, milk and dairy products, shrimp, salad dressing, cocoa, chocolate,

and salad-type sandwich filling (such as tuna salad or chicken salad).

An important route of contamination is the handling of food by people who have not washed their hands properly after using the bathroom. This "fecal to oral" route of transmission can be prevented by hand washing, and proper kitchen hygiene (e.g., cleaning cutting boards after cutting raw poultry, storage of prepared foods in the refrigerator).

The thousands of different strains of Salmonella are also known as serotypes. These designations indicate that the differences between the strains lie mainly in the chemically different composition of the outer surface of the bacteria. The differences elicit different immune responses. The immune response for a particular strain is characteristic and can be useful in identifying the strain of Salmonella that is causing the malady. *Salmonella enteritidis* is of particular concern in food poisoning. This strain causes gastroenteritis and other maladies.

Strains like *Salmonella enteritidis* can establish infection because they have components that contribute to the infection. These components are classified as virulence factors. One of these factors is called adhesin. An adhesin functions in adhesion of the bacterium to a receptor on the surface of a host cell. An example of an adhesin is the tube-like structures called fimbriae that stick out from the surface of the cell.

Another virulence factor is lipopolysaccharide (LPS for short). LPS can help shield the surface of the bacterium from host antibacterial compounds. A part of the LPS called lipid A can cause a fever and a subcomponent of lipid A called endotoxin is harmful to the host. Salmonella also produces other toxins (e.g., enterotoxin). Because these toxins remain inside the bacterial cell, the increased number of bacteria that results from multiplication in the contaminated food increases the amount of the toxin ingested, and so increases the severity of symptoms.

The identification of Salmonella is not particularly difficult. Well-known lab media of defined composition exist, on which the bacteria grow and produce characteristic colours. For example, Salmonella grows on bismuth sulfide media and produces jet-black colonies, due to the production of hydrogen sulfide.

Unfortunately, however, the accurate diagnosis of Salmonella food poisoning usually comes after the fact, if the illness is diagnosed at all.

A vaccine that blocks the adhesion of the bacteria to the intestinal epithelial cells, which is a crucial part of the infection, could conceivably be developed. However, even if such a vaccine is possible, other vaccine needs that are more pressing currently occupy dedicated research resources. For the foreseeable future, the best strategy in preventing Salmonella food poisoning will remain the cooking of foods such as meat to the proper temperature for a recommended time, the proper storage of prepared foods, and good hygiene.

## ■ FURTHER READING:

### BOOKS:

Fox, Nicols. *Spoiled: Why Our Food Is Making Us Sick and What We Can Do about It*. New York: Penguin USA 1998.

Salyers, Abigail, A., and Dixie D. Whitt. *Bacterial Pathogenesis: A Molecular Approach*. Washington, DC: American Society for Microbiology Press, 2001.

### ELECTRONIC:

Centers for Disease Control and Prevention. "Salmonella Enteritidis." Division of Bacterial and Mycotic Diseases. April 25, 2001. <[http://www.cdc.gov/ncidod/dbmd/diseaseinfo/salment\\_g.htm](http://www.cdc.gov/ncidod/dbmd/diseaseinfo/salment_g.htm)>(08 March 2003).

United States Food and Drug Administration. "Salmonella spp." Center for Food Safety and Applied Nutrition. January 10, 2003. <<http://vm.cfsan.fda.gov/~mow/chap1.html>>(02 March 2003).

### SEE ALSO

*Bioterrorism*  
*Food supply, Counter-Terrorism*  
*Infectious disease, threats to security*  
*Pathogens*

## Sandia National Laboratories

### ■ K. LEE LERNER

Founded in 1949, Sandia National Laboratories, located in New Mexico (with additional laboratory facilities in California and Hawaii), is a government-owned facility managed by Lockheed Martin corporation for the Department of Energy (DOE). Sandia was originally managed by AT&T, but in 1993 Lockheed Martin assumed managerial control.

Sandia scientists and engineers participate in projects and programs designed to ensure the safety of the U.S. nuclear stockpile and maintain a high level of reliability in aging weapons. Increasingly key to safeguarding the nuclear stockpile is the development of high-speed virtual simulation capabilities that are able to model the complexities of the changes in weapons material as a function of time. Sandia programs also support the development of technologies and protocols that facilitate nonproliferation and secure control of nuclear materials (e.g., enhance weapon and surveillance technologies). Specific programs to enhance offsite monitoring include the advancement of robotics systems capable of monitoring proliferation activities.

Sandia supports programs seeking to assist Russia to safely manage and control nuclear materials from dismantled Soviet-era weapons systems.

Other less direct, but equally emphasized programs, are designed to enhance U.S. national security by developing technologies to protect critical infrastructure—especially energy production and delivery infrastructure.

A specific aim of current Sandia projects involves potential integration of pulsed power technologies into defense-related applications. Other programs related to infrastructure protection are dedicated to extending the protection levels of radiation-hardened microelectronics.

In an effort to combat emerging threats, Sandia scientists and engineers are tasked with anticipating the need for new defense options and for developing technology capable of identifying (and neutralizing) biological and chemical agents. One Sandia innovation, "Amazing foam," is a nonhazardous decontaminating foam capable of rapidly neutralizing both chemical and biological agents.

Another Sandia innovation, the "magic cube," is capable of shaping a blast that blows a fragment-free hole in steel. Such developments have broad application. Magic cubes can be used to enhance low-invasive inspection of steel encased materials or to blow a hole in steel beams obstructing rescuers attempting to search through rubble or reach victims of a building collapse.

Sandia also devotes research resources to advancing techniques involved with hazardous material clean-up and the safe decommissioning and dismantling of obsolete weapons. Scientists at Sandia National Laboratories California collaborated with researchers at Lawrence Berkeley National Laboratory and Lawrence Livermore National Laboratory on the development of environmental remediation technologies useful in the cleanup of military disposal sites (e.g., the nearby Alameda Naval Air Station).

Sandia's technology transfer programs (where facets of defense related research are released and shared with private industry) are designed to increase United States' global economic competitiveness. The transfer is a bilateral arrangement that also allows industry input in defense design schemes. Other public programs sponsored by Sandia include educational outreach programs designed to foster excellence in scientific curricula and teaching.

Sandia scientists and engineers are highly involved in nuclear weapons production. Sandia designs and engineering integration impact and more than 6,300 parts of the estimated 6,500 components of modern nuclear weapons. Other programs designed to enhance national security include highly specialized and sophisticated modeling and testing facilities that allow Sandia scientists to test updates to weapons systems without actual nuclear testing. Failsafe technologies—devoted to preventing accidental nuclear detonation—include sophisticated arming and firing systems (e.g., the MC2912 arming system utilized on the W76/Mk4 nuclear warhead).

Sandia's sensory technology programs are designed to detect nuclear materials as well as chemical and biological weapons agents.

Scientists at LBL, Lawrence Livermore National Laboratory (LLNL), and Sandia National Laboratories California have also collaborated on the development of environmental remediation technologies useful in the cleanup of



A Sandia National Laboratories researcher speaks by phone with someone inside an early model of the ultra-clean room invented in 1962. Sandia is also responsible for about 98 percent of the 6,000 non-nuclear parts in nuclear weapons. AP/WIDE WORLD PHOTOS.

military disposal sites (e.g., the nearby Alameda Naval Air Station).

In April 2003, Sandia scientists reported that they had achieved controlled thermonuclear fusion in a pulsed power source. If ultimately reproduced and verified, the process, and other competing approaches to controlled fusion, holds the promise of nearly unlimited clean power generation. Unlike fission reactions, fusion based energy technology would not produce long-lived radioactive waste.

Instead of using magnetic containment to compress hydrogen and thereby achieve temperatures hot enough for fusion to occur, Sandia scientists used pulsed releases of current to achieve a rapid series of limited micro fusion reactions. Using an improved and more powerful Z accelerator, high current is induced in a tungsten wire cage surrounding a 2 mm plastic capsule containing deuterium (a heavier isotope of hydrogen). The tungsten cage is vaporized, but the short-lived current impulse generated in the wires creates a powerful magnetic pulse and shockwave of superheated tungsten that creates an intense x-ray source that, along with the shockwave compresses

and heats the hydrogen to more than 20 million degrees Fahrenheit (more than 11 million degrees Celsius) to induce fusion.

The Sandia reaction process contrasts with another promising approach undertaken at the Lawrence Livermore National Laboratory (LLNL) that seeks to initiate fusion reactions by shining high-energy lasers on hydrogen globules. The LLNL approach will be further explored at the National Ignition Facility.

#### ■ FURTHER READING:

##### ELECTRONIC:

United States Department of Energy, Office of Science. National Laboratories and User Facilities. <[http://www.sc.doe.gov/Sub/Organization/Map/national\\_labs\\_and\\_userfacilities.htm](http://www.sc.doe.gov/Sub/Organization/Map/national_labs_and_userfacilities.htm)> (March 23, 2003).

United States Department of Homeland Security. Research & Technology. <<http://www.dhs.gov/dhspublic/display?theme=27&content=374>> (March 23, 2003).



## SEE ALSO

Argonne National Laboratory  
 Brookhaven National Laboratory  
 DOE (United States Department of Energy)  
 Environmental Measurements Laboratory  
 Lawrence Berkeley National Laboratory  
 Lawrence Livermore National Laboratory (LLNL)  
 Los Alamos National Laboratory  
 NNSA (United States National Nuclear Security Administration)  
 Oak Ridge National Laboratory (ORNL)  
 Pacific Northwest National Laboratory  
 Plum Island Animal Disease Center

---

## Sarin Gas

---

■ JULI BERWALD

Sarin gas (O-Isopropyl methylphosphonofluoridate), also called GB, is one of the most dangerous and toxic chemicals known. It belongs to a class of chemical weapons known as nerve agents, all of which are organophosphates.

The G nerve agents, including tabun, sarin and soman, are all extremely toxic, but not very persistent in the environment. Pure sarin is a colorless and odorless gas, and since it is extremely volatile, and can spread quickly through the air. A lethal dose of sarin is about 0.5 milligrams; it is approximately 500 times more deadly than cyanide.

**History and global production of sarin.** Sarin was first synthesized in 1938 by a group of German scientists researching new pesticides. Its name is derived from the names of the chemists involved in its creation: Schrader, Ambros, Rudriger, and van der Linde. A pilot plant to study the use of sarin was built in Dyernfurth. Although they produced between 500 kg and 10 tons of sarin, the German government decided not to use chemical weapons in artillery during World War II. The Soviet army captured the plant at Dyernfurth at the end of the war and resumed production of sarin in 1946. The Russian government currently has about 11,700 tons of sarin.

Between about 1950 and 1956, the United States produced sarin. It is estimated to have stockpiles totaling 5,000 tons of the nerve agent stored in different parts of the country. Several other countries including Syria, Egypt,



Subway passengers affected by sarin gas planted in central Tokyo subways are carried to the hospital in March 1995. Years after the Aum Shinri cult's terrorist attack in which 11 people were killed and thousands were injured, many victims still suffer physical symptoms from the gas. AP/WIDE WORLD PHOTOS.

Iran, Libya, North Korea, and Iraq have confirmed or suspects stocks of sarin.

**Sarin as a weapon.** Iraq produced sarin between 1984 and 1985, when weapons inspectors were ordered to leave the country. Prior to Operation Iraqi Freedom, Iraq had admitted to once having at least 790 tons of the nerve agent. In 1987 and 1988, the United Nations confirmed that Iraq used a combination of organo-phosphorous nerve agents against Kurds in northern Iraq. It is estimated that 5,000 people were killed and 65,000 others were wounded in these attacks. There was also extreme environmental damage.

On March 20, 1995, the Aum Shinrikyo doomsday cult released the nerve agent sarin in a Tokyo subway. This incident killed 11 and injured more than 5,500 people. Members of the cult left soft drink containers and lunch boxes filled with the toxin on the floor of subway trains. They punctured the containers with umbrellas just as they exited the cars. The attack was timed for rush hour, so as to affect as many people as possible. Because the sarin was of low quality and the affected cars were quickly sealed once the sarin was detected, the magnitude of the attack was suppressed.

**Sarin poisoning.** Like other organophosphate nerve agents, sarin inhibits the break down of the enzyme acetylcholinesterase. Under normal conditions, this enzyme hydrolyzes the neurotransmitter acetylcholine. When sarin is present, the build up of acetylcholinesterase results in the accumulation of excessive concentrations of acetylcholine in nerve synapses. This overstimulates parasympathetic nerves in the smooth muscle of the eyes, respiratory tract, gastrointestinal tract, sweat glands, cardiac muscles, and blood vessels.

After exposure to sarin, symptoms begin within minutes. If a person survives for a few hours after exposure, he or she will likely recover from the poisoning. The first symptoms of sarin poisoning include a runny nose, blurred vision, sweating, and muscle twitches. Longer exposures result in tightness of the chest, headache, cramps, nausea, vomiting, involuntary defecation and urination, convulsions, coma, and respiratory arrest.

Atropine acts an antidote for nerve agent, including sarin. Atropine binds to one type of acetylcholine receptor on the post-synaptic nerve. A second antidote is pralidoxime iodide (PAM), which blocks sarin from binding to any free acetylcholinesterase. Both should be administered as soon as possible following exposure to the toxin. Diazepam can also be used to prevent seizures and convulsions. Soldiers fighting in regions where chemical weapons are likely to be deployed are now equipped with a Mark I antidote kit containing both atropine and PAM.

## ■ FURTHER READING

### ELECTRONIC:

Centers for Disease Control and Prevention: "Facts About Sarin" <<http://www.bt.cdc.gov/agent/sarin/basics/facts.asp>> (March 25, 2003).

Council on Foreign Relations: Terrorism Questions and Answers, "Sarin" <<http://www.terrorismanswers.com/weapons/sarin.html>> (March 25, 2003).

"Sarin Poisoning on Tokyo Subway" <<http://www.sma.org/smj/97june3.htm>> (March 25, 2003).

### SEE ALSO

*Biological Warfare*  
*Nerve Gas*  
*Toxins*

## SARS (Severe Acute Respiratory Syndrome).

SEE *Communicable Diseases, Isolation, and Quarantine.*

---

# Satellite Technology Exports to the People's Republic of China (PRC)

---

## ■ JUDSON KNIGHT

The issue of satellite technology exports from the United States to the People's Republic of China (PRC) mirrored larger concerns over Chinese espionage that surfaced in the late 1990s. In the case of satellite technology sales, however, United States companies and even some sectors of the federal government favored at least some degree of technology transfer, if only to maintain good relations between the two countries. This was particularly the case after September 11, 2001, as President George W. Bush sought to establish stronger ties with the Chinese in the fight against terrorism. Still, questions remained regarding the advisability of some such transfers, as well as the legality of transfers that had taken place in the mid-1990s and later.

**Allegations in the 1990s.** During the administration of President William J. Clinton, a number of critics charged that the president had been involved in a scheme to channel funds from the PRC to the Democratic National Committee. Clinton's defenders dismissed the criticism as a partisan attack from the far Right, and while most of the

critics were conservatives, not all of them could be dismissed as extremists. An example was the respected columnist William Safire, who wrote in the *New York Times* on May 18, 1998, that “A president hungry for money to finance his re-election overruled the Pentagon; he sold to a Chinese military intelligence front the technology that defense experts argued would give Beijing the capacity to blind our spy satellites and launch a sneak attack.” Complicit Democrats in the Senate, Safire and others charged, had blocked efforts to investigate the illegal transfer of technology.

One particular point of contention was the fact that Clinton had given the Department of Commerce increased jurisdiction over satellite technology transfers. This was significant in light of allegations that a Commerce official, John Huang, had ties to the Chinese. The sale of satellite communications technology to China had first been permitted by President Ronald Reagan, who in September 1988 negotiated a bilateral agreement with the PRC to ensure that no missile or satellite technology was transferred. Over the next four years, the State Department licensed all communications satellites, but as a result of a review conducted by the administration of President George Bush in 1990, licensing jurisdiction for purely commercial satellites was transferred to Commerce. Franklin C. Miller, Principal Assistant Secretary of Defense for Strategy and Threat Reduction, testified before the Senate Committee on Commerce, Science, and Transportation in September 1998, that Defense had supported this act because it “was accompanied by several changes in procedures that protect Department of Defense’s ability to ensure that transfers are consistent with U.S. national security.”

Despite this testimony, Henry Sokolski of the Nonproliferation Policy Education Center maintained that Clinton had gone much further than his predecessors. In testimony before a joint hearing of the House International Relations Committee and the House National Security Committee in June 1998, he maintained that “this shift has eliminated systematic government monitoring of prelaunch conversations between U.S. contractors and Chinese space firms and, according to the General Accounting Office, marginalized the previously important licensing input of the Defense Department.” As though to underscore Sokolski’s point, it was later revealed that in 1996, Loral Space & Communications Corporation had forwarded a report on a Chinese rocket to the Chinese government without first obtaining State Department clearance, a situation that led to a grand jury investigation.

**A change of course in the 2000s.** A concern similar to that involving Loral erupted in late 2002, when the State Department accused Hughes Electronic Corporation of providing the Chinese with key information to assist them in determining why their rockets tended to fail soon after launch. The incident had occurred in the 1990s, according to the State Department—in other words, at the high point of

concerns over the transfer of sensitive satellite technology to the PRC. Although the State Department threatened fines of up to \$60 million, by the time the charges came to light, the situation with regard to satellite technology transfers to the PRC had changed.

This change did not so much involve security as it did commerce—specifically, an increased demand by U.S. aerospace companies to relax restrictions on transfers. The change created some strange political bedfellows: joining fellow California representative Howard L. Berman, a Democrat, in putting forward the proposal was Dana Rohrbacher, a Republican who had opposed the Clinton-era transfer of licensing authority to Commerce. Yet, in 2001, Rohrbacher—whose constituency, like that of Berman, had a strong aerospace presence—supported the very measure he had condemned three years earlier. Just as Berman and Rohrbacher constituted a bipartisan team, they found themselves opposed from both sides of the aisle. Not only Republican senators Jesse Helms and Richard Shelby, but also Democratic representative Tom Lantos of California, maintained that the move posed security risks.

By that time, however, the tides had shifted, and the move to increase sales of satellite technology to China gained momentum. In April 2002 the State Department loosened rules on export of scientific satellite projects to the PRC. Six months later, as Chinese head of state Jiang Zemin met with President George W. Bush at the latter’s ranch in Texas, the two discussed the possibility of easing bans on the transfer of satellite technology, provided China reduced its sales of missile technology to third parties. The leaders did not reach an agreement, however, and debate continued. On March 28, 2003, during the U.S. military effort against Iraq, a missile fired by the Iraqis hit a shopping mall in Kuwait, a country aligned with the United States in the war. The weapon was a modified Chinese-made Silkworm rocket.

#### ■ FURTHER READING:

##### PERIODICALS:

- Lawler, Andrew. “Rules Eased on Satellite Projects.” *Science*. 296, no. 5566 (April 12, 2002): 237–238.
- Marquand, Robert. “As War Looms, U.S. Talks to China.” *Christian Science Monitor*. (October 21, 2002): 6.
- Marquis, Christopher. “Some Lawmakers Urging U.S. to Speed Exports of Satellites.” *New York Times*. (July 9, 2001): A7.
- Safire, William. “China Syndrome: Clinton’s Greed for Funds Triggers a Security Meltdown.” *New York Times*. (May 18, 1998): A19.

##### ELECTRONIC:

- Defense DAS Miller on Technology Transfers to China. U.S. Department of State. <<http://usinfo.state.gov/regional/ea/uschina/millr917.htm>> (March 29, 2003).

Sokolski, Henry. U.S. Satellite Technology Transfers to China: What's at Issue, Questions and Answers. Non-proliferation Policy Education Center. <[http://www.npec-web.org/presentations/sat\\_trans.htm](http://www.npec-web.org/presentations/sat_trans.htm)> (March 29, 2003).

#### SEE ALSO

*Chinese Espionage against the United States Satellites, Non-Governmental High Resolution Satellites, Spy*

## Satellites, Non-Governmental High Resolution

■ WILLIAM C. HANEBERG

Satellite imagery at resolutions useful for military and intelligence purposes has historically been available only from satellites developed, launched, and operated by governments. As a result, access to and dissemination of the high-resolution satellite images was tightly controlled in the interest of national security. Since 1999, however, commercial satellites have made high-resolution images publicly available at a relatively low cost. In the United States, the Land Remote Sensing Policy Act of 1992, which was motivated in part by Russian willingness to sell declassified 2 m resolution military satellite imagery in the early 1990s, provided the legal foundation for private ownership of American remote sensing satellites. In 1994, the Clinton administration issued guidelines for the licensing of commercial remote sensing satellite operations.

The resolution of an image is the size of the smallest object that can be depicted, and the best images currently available from commercial satellites have resolutions ranging from 50 cm to 1 m. Imagery from the most recent intelligence satellites launched by the United States government, in contrast, is believed to have a resolution of about 2 cm. No images with this resolution, however, have been released to the public. Although there is no universally accepted definition of "high resolution," in part because its meaning changes as technology improves, at the time this article was written it was generally understood to mean resolutions of 2 m or less.

IKONOS, named after the Greek word for "image," was the first commercial satellite to provide images with 1 m resolution. Its products include 1 m panchromatic (black and white) and true color images in addition to 4 m multispectral imagery. Following a sun-synchronous orbit 680 km above Earth's surface, IKONOS passes over any given longitude at about 10:30 a.m. local time each day and revisits any given geographic location every three days. Space Imaging, the company that operates IKONOS



A satellite image showing the Yongbyon nuclear facility in North Korea taken in 2002. According to the Institute for Science and International Security (ISIS), significant facilities in the image include a five-megawatt reactor and cooling tower, and a spent fuel storage building in the bottom of the site near the river. AP/WIDE WORLD PHOTOS.

was founded by a consortium of firms from the United States, Japan, and South Korea. The satellite was launched in August 1999 after the first version was destroyed when its launch vehicle malfunctioned and crashed the previous spring.

Developed by an international consortium of companies based in Cyprus and known as ImageSat International (ISI), the EROS A1 satellite was built largely in Israel and launched in 2001 from a Russian facility in Siberia. It was the first high-resolution commercial satellite developed outside of the United States. The EROS A1 camera, which can provide 1.8 m resolution panchromatic images, is



A view of the port and downtown areas of Abu Dhabi made by the QuickBird satellite provided by DigitalGlobe. QuickBird snaps some of the most detailed satellite images available to the public. AP/WIDE WORLD PHOTOS.

based on technology originally developed for Israeli intelligence satellites. The successor the EROS A1, known as the EROS B1, is scheduled for launch in late 2004 and is expected to produce both panchromatic and multi-spectral color imagery with 0.87 m resolution.

The highest resolution commercial imaging satellite currently in operation is QuickBird, operated by the Colorado-based firm Digital Globe, which follows a sun-synchronous orbit 450 km above Earth. The first QuickBird was lost in space after a late 2000 launch from a Russian facility in Siberia. A replacement was successfully launched

from Vandenberg Air Force Base, California, atop a Delta II launch vehicle in late 2001. QuickBird supplies 0.62 m resolution panchromatic images and 2.4 resolution multispectral color images.

Proponents of commercial high-resolution imaging satellites argue that their images will be useful for a variety of civil work that includes infrastructure monitoring, natural disaster recovery, endangered species habitat identification and monitoring, and natural resource exploration. Commercially available high-resolution images can also be used to monitor troop and equipment movement,

observe construction activity, identify targets in inaccessible areas, and remotely assess battle damage. This has led the United States government to prohibit its licensees from obtaining or selling high-resolution imagery of Israeli territory in response to concerns raised by the government of Israel. It also reserves the right to restrict operations during times of national security emergencies. These restrictions do not apply, however, to commercial satellites operated by companies outside of the United States.

#### ■ FURTHER READING:

##### BOOKS:

Bossler, John D., John R. Jensen, Chris McMaster, and Chris Rizos (editors). *Manual of Geospatial Science and Technology*. Mount Laurel, New Jersey: Taylor & Francis, 2001.

Campbell, James B. *Introduction to Remote Sensing (3rd edition)*. New York: Guilford Press, 2002.

##### ELECTRONIC:

Baker, J.C. "Commercial Observation Satellites: A Catalyst for Global Transparency." 2002. <<http://www.imagingnotes.com/julaug01/global.htm>> (12 April 2003).

"Digital Globe." <<http://www.digitalglobe.com/>> (12 April 2003).

"ImageSat International." 2003. <<http://www.imagesatintl.com/>> (12 April 2003).

"Space Imaging—Visual Products. Visible Results." 2003. <<http://www.spaceimaging.com/>>(12 April 2003).

##### SEE ALSO

*Cameras*

*Geospatial Imagery*

*LIDAR (Light Detection and Ranging)*

*Photographic Resolution*

*Photography, High-Altitude*

*Remote Sensing*

## Satellites, Spy

■ LARRY GILMAN

Spy satellites are robotic observational platforms that orbit the Earth in order to image its surface and to record radio signals for military and political purposes. They transmit their data to Earth, where it is interpreted by specialists in centralized, secretive facilities such as the U.S. National Photographic Interpretation Center in Washington, D.C. Spy satellites have been essential not only to military operations and the formation of national policy but to the verification of arms control treaties such as SALT I, SALT II, and the Comprehensive Test Ban Treaty.

Hundreds of spy satellites have been launched since 1960, when the U.S. lofted its first. The four basic types of spy satellite are: (1) photoreconnaissance systems that



Israel launched the Ofek-5 spy satellite at a coastal air force base south of Tel Aviv in 2002 to extend its ability to monitor developments in the region. AP/WIDE WORLD PHOTOS.

take pictures in visible and infrared light, (2) infrared telescopes designed to detect missile launches, (3) radars that image sea or land even through cloud cover and in darkness, and (4) signals intelligence (SIGINT) satellites (also termed "ferrets"), which are optimized either for characterizing ground-based radar systems or for eavesdropping on communications. Sometimes photoreconnaissance and SIGINT functions are combined in single, massive platforms such as the U.S. Keyhole-series satellites.

Although a number of nations have launched spy satellites, the U.S. and the Soviet Union are responsible for by far the greatest number. The Russian Federation, which inherited most of the Soviet Union's space system after 1991, has been unable to afford the cost of adequately updating its spy satellite network. In contrast, the U.S. has continued to deploy ever-more-sophisticated systems in a steady stream. Thus, the majority of spy satellites in orbit today, including all the most capable units, are U.S.-owned. Although the precise technical capabilities (and in many cases even the basic missions and orbits) of U.S. spy satellites are secret, it is thought that the best U.S. visible-light spy satellites are capable, given

clear skies, of imaging surface features only a few centimeters across. A modern U.S. spy satellite can, given clear skies and a good viewing angle, probably read a license plate from space.

## Early U.S. Spy Satellites: Corona, MIDAS, SAMOS

The U.S. began developing spy satellites in the mid-1950s, years before it had a rocket capable of placing anything in orbit. As early as 1946, RAND (short for the RAND or *Research and Development Corporations*, a think tank created by Douglas Aircraft Co. that was influential throughout the Cold War) had produced a report entitled "Preliminary Design of an Experimental World-Circling Spaceship." The usefulness of such systems was obvious long before they were buildable, for military forces had been seeking higher vantage points from which to observe the enemy ever since the U.S. Civil War, when the Union experimented with tethered observation balloons overlooking Confederate positions. In the early twentieth century, reconnaissance blossomed when photographic film replaced cumbersome glass plates and cameras were borne aloft on aircraft. So effective is aerial photography that it is still used today; the U.S., for example, continues to employ its high-altitude U-2 and SR-71 Blackbird aircraft, early versions of which it developed in the 1950s and 1960s.

However, spy planes have limitations. Even the highest-flying airplane cannot fly above the atmosphere, and can therefore, view only a limited amount of ground at any one time. Even at four times the speed of sound (the approximate top speed of an SR-71), this is a severe disadvantage when trying to surveil a country as large as China or Russia. Nor can planes be kept aloft indefinitely; they must be sent out at intervals. They must also be piloted, putting crew members at risk of death or capture. This was illustrated most famously in 1960, when CIA pilot Gary Powers was shot down while flying a U-2 spy plane over the Soviet Union and tried for espionage. (In recent years, robotic aircraft have been employed for some short-range aerial reconnaissance.) Finally, spy planes are intrinsically illegal in time of peace—they must violate national airspace to do their job—and therefore, a political liability.

Spy satellites overcome all the limitations of spy planes. A network of three geosynchronous satellites can, in contrast to the occasional glimpses provided by spy planes, keep the entire world in view at all times. (A geosynchronous satellite orbits 22,160 mi [35,663 km] above the equator in the direction of the Earth's rotation, matching its movement with the Earth's surface so that it appears to hover at a fixed point in the sky.) A network of lower-altitude satellites in polar orbits (i.e., circling at right angles to the equator, over the poles) can, by combining their smaller fields of view, do the same. Also, satellites

are at an altitude too high to be easily shot down, though the U.S. and Russia have developed anti-satellite weapons in case they should ever wish to do so. Finally, satellites are legal: they do not violate national airspace. This legal point was not always universally acknowledged; for a few months in 1960 the Soviet Union complained that U.S. spy satellites were violating its airspace, which, it said, extended upward indefinitely from its territory. It dropped this argument when it began launching its own spy satellites in October, several months after the United States.

The U.S. Air Force and Central Intelligence Agency (CIA) were early advocates of satellite surveillance. ("Surveillance," strictly speaking, refers to the passive, ongoing observation of some area to scan for activities or changes of interest, while "reconnaissance" refers to the active seeking of specific information at a particular time; however, the word "surveillance" is often used to cover both activities.) A detailed study released by RAND in 1954 suggested two basic methods for returning imagery to Earth from an orbiting platform: (1) television pictures scanned from photographic film on board a spacecraft and beamed to Earth, and (2) return of the film itself to Earth in a reentry vehicle. The Air Force decided to develop the first option, arguing that retrieving film from space would be time-consuming and unreliable; the CIA decided to develop the second, reasoning that TV technology was still too crude to give sufficiently high-resolution pictures.

Squabbling between the Air Force and CIA, both jockeying for control of U.S. space surveillance resources, eventually moved President Dwight Eisenhower to create the National Reconnaissance Office (NRO) on August 25, 1960. Then NRO (officially secret until the early 1990s) is staffed by personnel from the Air Force, CIA, and other government agencies and is charged with overseeing the United States's space-surveillance programs. Under the NRO's guidance, three major spy-satellite programs went ahead in the early 1960s, one directed by the CIA and two by the Air Force.

The CIA's system, code-named Corona, took high-resolution photographic negatives with orbiting telescopic cameras and then dropped them to the Earth. The first 12 attempts to achieve orbit or return film all failed, but starting with Corona 13 in August, 1960, Corona began to fulfill its promise. A long series of Corona satellites were launched, orbited over the Soviet Union, and returned their exposed film in reentry capsules. Each capsule deployed a parachute after it had killed most of its velocity by friction with the atmosphere, and was then hooked from the air by a propeller-driven JC-130B aircraft flying at about 150 miles per hour (242 km/hr). The Corona satellites returned excellent images, with later models probably achieving a resolution of about 1 foot (.3 m). One of Corona's first achievements was to debunk the Air Force's claims that a huge "missile gap" existed in the early 1960s between the Soviet Union and the U.S.—that is, that the



Soviets many more ICBMs (intercontinental ballistic missiles) than the U.S. In fact, as Corona showed, the Soviets actually had far fewer missiles than the U.S. at that time.

Because each Corona satellite had a limited film supply, it remained in orbit only for hours or a few days, requiring that a new Corona be launched each time a new set of photographs was desired. Corona, therefore, did not keep the Soviet Union under constant surveillance, but instead ran a series of reconnaissance missions with specific goals. Over 120 Corona satellites were flown before being replaced in the early 1970s by the larger and more sophisticated film-return satellite known as KH-9 HEXAGON (or “Big Bird”).

The two spy-satellite programs pursued by the U.S. Air Force in the early 1960s were SAMOS (Satellite and Missile Observation System) and MIDAS (Missile Alarm Defense System). SAMOS satellites took pictures on film, developed the film in orbit, and transmitted TV scans of the pictures to Earth. Because the TV pictures were much blurrier than the film, SAMOS had low resolution even for its day (5–20 feet), and some authorities (e.g., Herbert Scoville, Jr. [1915–1985], arms-control expert and one-time CIA analyst) have claimed that SAMOS never produced useful data. It was not until the 1970s, with the launch of the KH-11 spy satellite (discussed further below), that radio return of data from orbit was to provide images as good as those available directly from film. The first successful SAMOS launch was on January 31, 1961; 26 more SAMOS satellites were launched between then and November 27, 1963, when the program ended.

Meanwhile, the Soviet Union was launching its own series of low-orbit photoreconnaissance satellites, the Cosmos platforms. Like Corona, the Cosmos satellites were film-return missions—a technique that the Soviet Union (and, later, the Russian Federation) would continue to use until 2000, when the Enisei satellite, designed to return high-resolution digital images in real time like the United States’s KH-11 and KH-12 satellites, was launched. The Cosmos were modified Vostok capsules originally designed to carry cosmonauts, rather than specialized platforms. (Later, the Soviets would also modify their larger Soyuz capsules for use as robotic spy satellites). Use of Vostok capsules had the advantage that the Soviets did not have to invent a separate film-return system, having already developed techniques for landing Vostok capsules by parachute.

Corona, SAMOS, and Cosmos followed polar orbits at altitudes of about 150 miles, circling Earth every 90 minutes or so. (Satellites at lower altitudes get a closer view but encounter atmospheric drag that shortens their lifetimes, eventually burning them up like meteors; spy satellites have been orbited as low as 76 miles, but they did not last long.) A polar-orbiting photoreconnaissance satellite views a limited portion of the surface at any one time, although its field of view moves rapidly over the Earth as the satellite speeds through space. MIDAS, the U.S. Air Force’s other early spy-satellite project, was different. Each MIDAS satellite was stationed at a much

altitudes (e.g., 2170 mi [3500 km]), from which it could see most or all of the Soviet Union at any moment. The MIDAS satellites were designed not to take visible-light images of the Earth, but to observe it in the infrared band of the electromagnetic spectrum. The goal was to detect the heat radiation (infrared light) given off by missile and rocket launches; MIDAS could radio warning of an attack to Earth long before ground-based radars could detect approaching missiles. Twelve attempts to orbit MIDAS satellites were made between February, 1960, and October, 1966. Most failed, but experience with MIDAS made possible its successor, the Defense Support Program (DSP) system of geosynchronous infrared early-warning satellites.

## Defense Support Program

The first DSP early-warning satellite was launched in 1970, the nineteenth in 1999. Unlike their predecessors, the MIDAS satellites, DSP satellites are deployed to geosynchronous orbits. Five are usually in operation at any one time: the three newest are used to observe parts of the Earth deemed most likely to be missile launch sites (e.g., Russia), while the two oldest are used both to observe less-critical areas and as backups for the first three. When a new DSP satellite is launched, the most obsolete of the five already in orbit is nudged by its rockets to a higher orbit in order to avoid cluttering the geosynchronous altitude.

DSP satellites combine high resolution with wide-area coverage by a mechanical trick. The field-of-view of a DSP satellite’s telescope is much smaller than the disk of the Earth, but the telescope is mounted at a slight angle to the long axis of the satellite, which is caused to spin at .175 revolutions per second. The working satellite thus resembles a rolling bottle with an off-angle straw protruding from its mouth, where the straw corresponds to the telescope and is pointed toward Earth. The telescope’s field of view is wobbled systematically over a larger area of the Earth than it would view if the satellite were stationary.

The data collected by DSP satellites are compressed by on-board computers and then transmitted to a data-collection station at Nurrungar, Australia, where they are analyzed in real time. This system underwent an unplanned but crucial test in 1979, when a computer tape simulating an all-out Soviet nuclear attack was mistakenly fed into the early-warning system of the U.S. Strategic Air Command’s control center in Colorado. Controllers assumed that a real attack was occurring, and U.S. ballistic-missile crews prepared to launch in retaliation. War was averted because U.S. leaders took the precautionary step of viewing real-time data from the DSP satellite system, which showed that no launches had actually occurred in the Soviet Union.

The Soviet Union, although always lagging the U.S. technologically, has also deployed infrared early-warning satellites. By the early 1990s, it had several “Prognoz” satellites in geosynchronous orbits doing the same job as the United States’s DSP satellites. It also had a collection of nine “Oko” (Russian for “eye”) satellites, also infrared



early-warning platforms, in elliptical (off-center) orbits. The latter were designed to observe the missile fields of the continental U.S. at a grazing angle. The advantage of such a view for early warning is that U.S. missiles would, within seconds of liftoff, be silhouetted against the blackness of space, making them easier to detect. Today, only one Prognost early-warning infrared satellite remains operational. To decrease the likelihood of a Russian ballistic-missile launch due to flawed or inadequate information, some experts have proposed that the U.S. and Russia set up a joint early-warning center where the U.S. would share its DSP data with Russian observers.

**Keyhole.** Since March, 1962, all U.S. photographic intelligence satellites and aircraft have been managed under the program name “Keyhole.” Keyhole satellite designs are given Keyhole numbers; SAMOS and Corona were retrospectively labeled KH-1 and KH-4. (There seems not to have been a KH-2 or KH-3.)

A dozen Keyhole satellite designs have been orbited to date, each generation containing a significant improvement over its predecessor. In the days when each satellite (whether a “bucket dropper”—film-return—type or TV-scanning type) carried a finite supply of photographic film, satellite lifespans were short and large numbers of each type were launched. For example, 46 copies of the KH-5 satellite (the immediate successor to the Air Force’s SAMOS) were launched from 1963 to 1967. Thirty-six copies of Corona’s successor, the KH-6, were orbited during the same period. The two satellite types were used in conjunction; low-resolution, wide-area images from a KH-5 would be used to identify targets for high-resolution, “close-look” reconnaissance by a KH-6.

The next close-look satellite, the KH-8 (still a bucket-dropper), was the first spy satellite to examine bands of the electromagnetic spectrum other than the visual-light band. Since the KH-8, all Keyhole satellites have examined light in several narrow bands in the visible and infrared parts of the spectrum. This is done in order to extract maximum information about ground features. A different lens must be used for each wavelength, as a single lens cannot focus all wavelengths simultaneously. This adds to the complexity and cost of each satellite, but increases its usefulness greatly.

The most famous Keyhole satellite type is the KH-11, the primary U.S. orbital imaging platform from 1976 to 1992 (when it was succeeded by the KH-12, still in service today). The KH-11 finally achieved the ambition of SAMOS’s designers: to return film-quality images from orbit electronically, without bucket-dropping. The invention of the charge-coupled device (CCD) in 1970 was key to this advance, and has transformed astronomy as well. A CCD is a microchip (i.e., a thin rectangle consisting mostly of silicon or another semiconductor,  $>.5 \text{ in}^2$ ); one side of the chip is an array of thousands of microscopic electronic devices that record photon impacts as electrical charges.

(A photon is the minimum unit of light.) Placing a CCD in the focal plane of a telescope and periodically reading off the contents of its array of photon sensors produces a digital image record. The CCD is thus the equivalent of the film in a conventional camera, with the difference that a CCD can be re-used indefinitely.

The image information from a CCD is stored in digital form. Digital information, unlike the analog TV signals from the original SAMOS, is easy to encrypt and to transmit without loss of quality. Furthermore, the abandonment of bucket-dropping meant that spy satellites could remain in orbit for years rather than weeks. This, in turn, has made it feasible to invest more money in each satellite, making it more complex and capable. (A modern KH satellite costs about a billion dollars.) SIGINT antennas were added to KH-11s as the series progressed, to eavesdrop on communications.

KH-11 and KH-12 satellites are also highly maneuverable. A KH-12 satellite carries some seven tons of hydrazine fuel with which to maintain its orbital altitude against atmospheric drag or to change its orbit in order to better view specific parts of the Earth.

**SIGINT and ferrets.** Signals intelligence (SIGINT) is divided into three sub-fields: communications intelligence (COMINT, the interception of messages), electronics intelligence (ELINT, the gathering of information about radar, radar jammers, and the like), and telemetry intelligence (TELINT).

TELINT is in fact a special type of COMINT. Telemetry is data about physical quantities measured by automatic devices, often embedded in missiles, spacecraft, or aircraft. When a new ballistic missile is tested, say by China, it radios a complex telemetry stream to the ground from the moment of its launch until it crashes or explodes. The telemetry stream is intended to show the missile’s designers exactly how the new machine is performing and, if it fails, what components caused the failure. (As a famous unclassified example, analysis of routinely-recorded telemetry from the space shuttle *Columbia* was essential to understanding the causes of that spacecraft’s explosion during reentry in 2003.) The telemetry—once decoded, a task accomplished by the U.S. National Security Agency (NSA) or a foreign equivalent—also reveals the detailed mechanics of the missile to TELINT eavesdroppers: fuel consumption, acceleration, guidance, and the like.

TELINT and COMINT collection are the primary missions of the U.S. Rhyolite series of satellites (also termed Aquacade), the first of which was launched in 1973. The Rhyolites are also thought to collect some ELINT (radar mapping data). Rhyolites must observe the Earth continuously in order to eavesdrop effectively on communications sessions, which usually last more than the few minutes that a fast-moving, low-altitude satellite is in range, and on telemetry from missile tests, which take

place at unpredictable times. They are therefore parked in geosynchronous orbits. Once in orbit, a Rhyolite unfolds a dish-shaped receiving antenna approximately 70 feet (21 m) across and begins listening. From its altitude of over 22,000 miles (35,400 km), a Rhyolite can pick up walkie-talkie conversations on Earth—and perhaps even weaker signals.

Other large, geosynchronous SIGINT satellites have been orbited by the U.S., with missions similar to Rhyolite's. Also, as mentioned above, the KH-11 and KH-12 series satellites have carried SIGINT as well as photoreconnaissance equipment. There is little that is transmitted electronically that cannot be intercepted by the United States's SIGINT satellites. The Soviet Union also launched numerous SIGINT satellites, emphasizing continuous coverage of the oceans and of North Atlantic Treaty Organization (NATO) countries by networks of low-orbiting satellites rather than by fewer, more sensitive satellites in geosynchronous orbits. Like other spy-satellite assets inherited by the Russian Federation from the Soviet Union, these SIGINT resources have degraded steadily, with many satellites falling out of service without replacement.

An important class of SIGINT satellites is dedicated to characterizing on-the-ground radar systems, including early-warning, missile-tracking, naval, civil, and other radars. Because radar systems are *designed* to radiate large amounts of electromagnetic energy, their detection is straightforward compared to the gathering of COMINT, and relatively small, cheap satellites suffice. Satellites or aircraft that specialize in characterizing enemy radars are termed "ferrets." Many ferrets have been launched since the first U.S. ferret in May 1962; some experts estimate that SIGINT satellites, including ferrets, are about four times as numerous as photoreconnaissance satellites. At least eight U.S. ferrets are orbiting the Earth at any one time, many in geosynchronous orbits or in highly elliptical orbits. The advantage of an elliptical orbit for ferreting is that when the satellite is near its apogee (i.e., when it is farthest from the Earth), its velocity is very low. By positioning the orbit so that its apogee is above an area of interest, Siberia, for example, the satellite can be made to "hang" for hours above that area, gathering continuous data. At the same time, elliptical orbits do not require as much energy to achieve as geosynchronous orbits, and so are cheaper.

**Radar Satellites.** Both the U.S. and the Soviet Union have launched satellites that map the Earth and track ships at sea using radar. Radar satellites, unlike visual-light satellites, can image at night and through clouds. Orbital radar imaging was first tested by the U.S. on a 1984 flight of the space shuttle *Challenger*, and was used with great success by the Magellan mission to Venus, launched 1989. Beginning in 2008, an ambitious U.S. program dubbed Discoverer II will orbit a constellation of low-orbit satellites called the Space-Based Radar (SBR) Objective System. The 24

satellites of the SBR Objective System will provide continuous, real-time, high-resolution radar imaging of the entire world, additionally supplying super-high-resolution imaging of a smaller area using side-looking synthetic-aperture radar (SAR). The ordinary radar footprint (area of view) of an SBR Objective System satellite will be a circle about the width of the continental United States; the footprint of its SAR will be about a quarter as large, shaped like a pair of butterfly wings aligned with the direction of travel of the satellite. These "wings" will slide along the ground with the satellite, defining a double track of territory that can be mapped by SAR. The SBR Objective System will provide real-time precision terrain mapping and tracking of vehicles moving on the ground, in the air, or at sea. (Radar cannot penetrate water, so submarines will not be observed.) Unlike older photoreconnaissance systems, which transmitted their information solely to centralized interpretation centers, information from the SBR Objective System will also be downlinked directly to commanders in the field. Testing of SBR Objective System satellite prototypes begin in 2004.

**Space-Based Infrared Satellite Systems.** An important U.S. satellite system that is now in the process of development is the Space-Based Infrared Satellite System (SBIRS), which is intended to replace the aging DSP early-warning system. SBIRS is intended not only to detect launches, but also to provide detailed tracking information that could be used in antiballistic missile defense. SBIRS will have two components, SBIRS High and SBIRS Low. SBIRS High will consist of satellites in geosynchronous and highly elliptical orbits, much like DSP, but with increased sensitivity. SBIRS Low will consist of a constellation of low-orbit satellites—probably 24, like the SBR Objective System—that will use infrared sensors to track missiles' trajectories for the purpose of guiding defensive systems such as interceptor missiles. Whether the proposed antiballistic missile system of which SBIRS Low would be a part would be effective is technically controversial. The first SBIRS High satellite was scheduled for launch in 2003, and the first SBIRS Low for about 2008.

**Other developments.** Although the U.S. and the Soviet Union had a monopoly on satellite launches during the 1960s, this began to change in 1970, when both China and Japan orbited their first satellites. Neither was a spy satellite: Japan had vowed to conduct a strictly nonmilitary space program, while the Chinese launch, like the Soviet Union's 1957 Sputnik, was a demonstration. (Its sole function was to broadcast a tape recording of the Chinese Communist anthem, "The East Is Red"). However, China was soon launching military satellites, and by 1999, claimed to possess a network of 17 spy satellites that monitor the U.S. military continuously. Japan launched its first two spy satellites in 2003, breaking its self-imposed ban on military space projects in order to spy on North Korea's

efforts to develop ballistic missiles and nuclear weapons. India launched its first spy satellite, the Technology Experiment Satellite (officially experimental, but viewed by space experts as a surveillance platform) in 2001.

Israel orbited its first spy satellite (Ofek 3, a photo-reconnaissance platform) in April 1995. For about one and a half years in 2000–2002, the demise of Ofek 3's successor, Ofek 4, left Israel without a national spy satellite system. During that period, it compensated by buying high-quality imagery from a civilian U.S. Earth-imaging satellite, Landsat. The quality of such imagery approaches that of the best spy-satellite imagery available to the U.S. or Soviet Union during the 1960s. As images from Landsat, Ikonos (a commercial U.S. satellite launched in 1999), and the French-owned SPOT (Système Probatoire d'Observation de la Terre) satellites are now available, anyone who can afford the per-image cost now has, in effect, significant satellite capability, whether for scientific or military purposes. Surveillance is in the eye of the beholder: an image is an image, whether produced by a "nonmilitary" or "spy" satellite. This was underlined during the U.S. war with Afghanistan in October 2001, when the U.S. government took the unprecedented step of buying exclusive rights to all Ikonos satellite images of Afghanistan in order to prevent them from being purchased by media outlets. It is likely that space imagery will continue to become more widely available as launch capabilities and imaging satellites proliferate, making it less feasible to control its distribution.

Just as nonmilitary orbital imaging systems are increasingly of military significance, military imaging systems are increasingly finding nonmilitary application. The DSP satellites have greatly augmented astronomers' catalogs of infrared stars. The SBIRS may be used to catalogue near-Earth asteroids to predict and possibly fend off a catastrophic collision; and after the loss of the space shuttle *Columbia* in 2003, NASA contracted with the U.S. National Imagery and Mapping Agency to routinely photograph shuttles in flight.

#### ■ FURTHER READING:

##### BOOKS:

Burrows, William E. *Deep Black: Space Espionage and National Security*. New York: Random House, 1986.

##### PERIODICALS:

Campbell, Duncan. "U.S. Buys up All Satellite War Images." *The Guardian (London)*, October 17, 2001.

Dooling, Dave. "Space Sentries." *IEEE Spectrum* (September, 1997): 50–59.

Duchak, G. D. "Discoverer II: A Space Architecture for Information Dominance." *Aerospace Conference Proceedings* (Vol. 7), IEEE, 1998: 9–17.

Forden, Geoffrey, Pavel Podvig, and Theodore A. Postol. "False Alarm, Nuclear Danger." *IEEE Spectrum* (March, 2000): 31–39.

Slatterly, James E., and Paul R. Cooley. "Space-Based Infrared Satellite System (SBIRS) Requirements Management." *Aerospace Conference Proceedings IEEE*, 1998: 223–32.

#### SEE ALSO

*Ballistic Missiles*

*Balloon Reconnaissance, History*

*Electronic Communication Intercepts, Legal Issues*

*Electro-Optical Intelligence*

*Geospatial Imagery*

*GIS*

*Global Communications, United States Office*

*IMINT (Imagery intelligence)*

*Intelligence and International Law*

*Mapping Technology*

*Photographic Interpretation Center (NPIC), United States National*

*Reconnaissance*

*Remote Sensing*

*Satellite Technology Exports to the People's Republic of China (PRC)*

*Satellites, Non-Governmental High Resolution*

*United States, Counter-terrorism Policy*

*Weapons of Mass Destruction, Detection*

## Saudi Arabia, Intelligence and Security

The Middle East is the seat of some of the world's most ancient civilizations and ethnic groups. Ancient Persia (Iran) and Byzantium (Turkey), in different eras, both claimed the land corresponding to present-day Saudi Arabia. These civilizations had complex government structures, which included developed bureaucracies and some of the earliest intelligence communities.

Abd al-Aziz Saud established the nation of Saudi Arabia in 1920 when he captured the city of Riyadh. He and his forces then began a three-decade campaign to unify tribal lands and city-states in the Arabian Peninsula. The quest was aided by the discovery of oil in the region during the 1930s, which produced great wealth for the royal family and Saudi Arabia. Today, the royal family remains in control of Saudi Arabia and the daily operations of its government. Because of its strategic location and its vast oil wealth, Saudi Arabia maintains one of the largest and most sophisticated intelligence communities in the Middle East.

In recent years, the Saudi government and intelligence services have become more concerned with the influx of refugees and immigrants. Increasing global concern over Islamist terrorist networks, and international suspicion of Saudi officials for permitting the funneling of

## Scanning Technologies

■ LARRY GILMAN

weapons and money through Saudi Arabia, prompted closer monitoring of Saudi national borders. Saudi intelligence and security forces erected video surveillance cameras, night vision and thermal cameras, and next-generation radar along national borders and the coastline. The electronic surveillance is meant to aid an extensive troop force, and free some military personnel for other operations. The government also offers incentives and high monetary awards for citizens who aid in the identification and arrest of illegal aliens.

Saudi civilian intelligence is directed by the Ministry of the Interior and Ministry of Interior Forces. The Directorate of Intelligence coordinates all civilian and some military intelligence operations. Both foreign and domestic intelligence information is collected and processed by the Directorate, which in turn works closely with Saudi Arabia's many police forces.

The Saudi government maintains several law enforcement agencies with ties to the intelligence community. The Directorate of Investigation investigates suspicious activity, conducts anti-terrorism and anti-crime surveillance, and has operational units to participate in security operations and political espionage. The Committees for the Propagation of Virtue and the Prevention of Vice (religious police) enforce the nation's tough anti-trafficking and drug laws, as well as social laws on modesty of dress and media censorship. The Public Security Police is the main national law enforcement agency, dedicated to preserving public safety and national security.

In addition to civilian forces, the Saudi military has extensive intelligence forces. The main agency for military and foreign intelligence is the G-2 Intelligence Section. The Ministry of Defense coordinates military intelligence and security operations, most of which are secret. Saudi military forces utilize the advanced surveillance and espionage technology in the region, gathering a wide range of electronic, signals, communications, remote, and human intelligence information.

In 1990 Saudi Arabia permitted the Kuwaiti royal family to flee the Iraqi invasion of Kuwait and establish an exile government in Saudi Arabia. In 1991 Saudi Arabia permitted the United States military to use its territory as a staging ground to launch an attack against Iraqi occupying forces in Kuwait in the Persian Gulf War. However, the Saudi government, at least publicly, opposed coalition military action against Iraq in 2003.

### ■ FURTHER READING :

#### ELECTRONIC:

Central Intelligence Agency. "CIA World Factbook, Saudi Arabia." <<http://www.cia.gov/cia/publications/factbook/geos/sa.html>> (March 29, 2003).

#### SEE ALSO

*Persian Gulf War*

X rays are electromagnetic waves in the  $10^{-8}$  to  $10^{-11}$  meter ( $3 \times 10^{16}$  to  $3 \times 10^{19}$  Hz) range of the spectrum. (Alternatively, x rays can, like all electromagnetic waves, be conceived of as particles termed "photons.") Because x rays have more energy than visible light, they can pass through solid objects that are otherwise opaque. However, they do not, in general, pass through them as if they almost transparent, as air is to visible light; rather, when x rays encounter materials of different densities and compositions, they are absorbed and deflected from their original straight-line paths (scattered) to different degrees. This allows x rays to be used for imaging the interiors of many objects. The two commonest commercial applications of x-ray scanning technology are medical imaging of the interior of the body and security scanning of baggage and cargo.

**Projection radiography.** Projection radiography (also termed transmission imaging or fluoroscopy), discovered in 1895, is the oldest and simplest form of x-ray scanning. In projection radiography, a beam of x rays is directed at an object behind which a detector or x-ray sensitive surface (i.e., electronic-device array or photographic film) is placed. Volumes of different absorptive properties in the object absorb and scatter the incident x rays to different degrees, causing an x ray shadow to be cast on the detecting surface. This shadow pattern is the x-ray image.

There are two essential limitations on projection radiography: first, it can readily resolve only structures that contain strong x-ray absorption contrasts. In human beings, this means that the soft tissues are difficult, or impossible, to image. Second, all three-dimensional structure in the x-rayed object is collapsed or flattened onto the image plane, destroying information. Nevertheless, because of their speed, simplicity, and economy, projection-type x-ray systems are still commonplace in hospitals and standard in security systems that examine cargo, baggage, and other inanimate objects. Airports rely heavily on projection-type x-ray machines to examine carry-on luggage and checked baggage for explosives and weapons. X raying of passengers, however, has until recently, been out of the question due to the negative health effects of x-ray radiation. X-ray photons are ionizing, that is, can knock electrons loose from atoms, disturbing whatever chemical bonds the atom may happen to be participating in. In a living system, ionization causes toxicity and genetic damage; at low levels it increases cancer risk and at high levels causes radiation sickness or death. At beam intensities high enough for rapid imaging of travelers, x rays would significantly increase long-term cancer risk. Fetuses and



A Transportation Security Administration screener, left, loads luggage into an x-ray scanner at the Bismark, North Dakota, airport. More than 30,000 new Security Administration employees were hired for increased airport security screening since the September 11, 2001, terrorist attacks on the World Trade Center in New York. AP/WIDE WORLD PHOTOS.

infants are especially vulnerable to all ionizing radiation, including x rays.

**Computed tomography.** Computed tomography (CT, also known as computerized axial tomography, CAT) was first made commercially available in the mid-1970s. CT combines projection radiography with computer processing to recover the three-dimensional information that is lost in a traditional two-dimensional x ray. In a CT scanner, the object to be scanned (e.g., person or baggage item) is placed in a cylindrical or doughnut-shaped device. Inside the cylinder or doughnut is an x-ray source that is mechanically rotated entirely around the object. Also, the cylinder or doughnut is lined with detectors that measure the x rays that pass through the scanned object at all angles. By collating all the information that is gathered during a full revolution of the x-ray source, a computer can form a three-dimensional model of the irradiated volume of the object. This information can then be presented to the user on a video screen in any desired form; most commonly, a thin slice of the object is modeled, with the details of its structure imaged as a black-and-white cross-section. To examine more of the object, the user looks at multiple slices.

CT scanning provides information not only on gross structure but on material density. In medical applications, this enables it to image soft tissues far better than conventional x-ray systems. In some security CT systems, the scanner's computer can automatically color-code densities characteristic of explosives or other special substances.

CT scanning is computation-intensive and requires rotation of the x-ray source around the scanned object, making this technique slower and much more expensive than transmission-type imaging. However, because CT images not only the geometry but the density distribution of complex three-dimensional structures, including (potentially) explosives shaped into thin sheets and other devices structured to avoid detection, most U.S. airports have one or more CT scanners. Since it is not practical to put all bags through the CT scanner, only selected or "suspicious" bags (e.g., those belonging to a passenger who pays cash for a one-way ticket) are passed through the CT scanner. Technological improvements in CT scanning are likely to make routine CT scanning of all luggage, with automated computer scanning for weapons or contraband, a reality at airports in some wealthy countries.

**Backscatter imaging.** “Backscatter” consists of waves that are reflected back from an obstacle. In backscatter imaging, x rays are beamed at a target object and a sensor co-located with the beam source records reflected (backscattered) waves. Since denser objects tend to create more backscatter, backscatter x-ray systems create a density-contrast image that reveals different information about objects’ interiors than does transmission imaging. Because transmission imaging and backscatter imaging can provide complementary information, relocatable military x-ray systems designed to inspect entire cargo containers, trucks, helicopters, and the like (e.g., the U.S. military’s Isearch system) acquire both transmission and backscatter images.

Backscatter imagers for personnel have also been constructed. A typical walk-through backscatter x-ray system can see what is beneath a person’s clothing—including the person. Although this is useful for detecting hidden weapons, it also raises obvious questions of privacy and legality where use on the general public, such as in airports, is proposed. There are also, as with all x-ray imaging modalities, health concerns. Although a walk-through of a backscatter imaging system would expose a person to only about 1/7,000 of the dose of a conventional medical x ray, some health physicists argue that frequent flyers and women who are pregnant but do not yet know it might still receive unacceptable cumulative doses from backscatter systems. (High-altitude air travel already increases a traveler’s exposure to x rays from space.) Backscatter x-ray systems have been deployed since the late 1990s in a few prisons as alternatives or aids to frisking, and have been found effective.

**Stereoscopic x-ray screening.** Using specially-constructed sensors it is possible to acquire transmission-type x ray information that can be formed into stereoscopic images (that is, a left-eye, right-eye image pair that the user’s brain combines into a three-dimensional impression). Because such an image has apparent depth but cannot be rotated, it is sometimes referred to as “2 1/2 dimensional.”

Stereoscopic x-ray technology is only a few years old, but may eventually replace conventional two-dimensional baggage scanners in airports because it provides the operator with additional visual-recognition cues that should increase their chances of correctly identifying weapons. Furthermore, stereoscopic x-ray scanning is quicker and cheaper than CT scanning, as it requires less computation and does not need to rotate the x-ray source around the object being scanned. Its limitations are that it provides neither fully rotatable three-dimensional knowledge of an object nor density data, both of which are provided by CT scanning.

**Coherent scattering.** The atomic orderliness of a substance affects the way in which x rays are diffracted (i.e., forced to mutually interfere) when passed through it. By recording the scattering patterns characteristic of specific compounds

(e.g., drugs, explosives), and comparing these templates to patterns observed when scanning objects, a substance-specific detection system can be devised. This technique is now in the early development stage, and is not ready for deployment.

**Other imaging modalities.** Several other techniques for imaging object interiors exist, including ultrasound, positron emission tomography (PET), nuclear magnetic resonance (NMR) imaging, nuclear quadrupole resonance (NQR) scanning, and neutron emission analysis. All, like x-ray scanning, have security, medical, or scientific applications; the question of which technique is best for any given application is decided based on physics (i.e., which imaging modalities can do a particular job) and, if more than one technique is usable for a given task, on economics (i.e., which imaging modality yields the minimum acceptable image quality for the least cost). For enhanced efficacy, airport security systems are now being planned that will combine complementary techniques to increase the probability of weapon or contraband detection. Such a system might combine x-ray scanning for suspicious-object detection with neutron emission analysis for chemical identification.

## ■ FURTHER READING

### PERIODICALS:

Bruning, Horst, and Stephen Wolff. “Automated Explosive Detection Systems Based Upon CT Technology.” *Security Technology* 1998. Proceedings., 32nd Annual 1998 International Carnahan Conference on. Oct. 12–14, 1998: 55–58.

Evans, J. P. O., M. Robinson, and S. X. Godber. “Pseudo-Tomographic X-Ray Imaging for Use in Aviation Security.” *IEEE AES Systems Magazine* July, 1998.

---

## SEAL Teams

---

Ranking among the most elite fighting forces in the world, United States Navy SEALs (Sea, Air, Land) operate in teams designed to wage unconventional warfare, particularly in a water environment. The SEAL team concept has its roots in World War II, though actual SEAL teams were not commissioned until 1962. SEAL training, conducted at the Naval Special Warfare Center in Coronado, California, is among the most rigorous programs of military education in the U.S. armed forces. SEAL team operations are noted for their mobility, swiftness, and precision.

In the spring of 1943, the U.S. Navy called for volunteers from its construction battalions (SeaBees) to form



U.S. Navy SEALs join their Filipino counterparts during a 2000 joint counter-terrorism exercise in a remote Philippine village, aimed at helping Philippine forces to destroy the Islamist extremist terror group Abu Sayyaf. AP/WIDE WORLD PHOTOS.

special naval combat demolition units whose mission was to reconnoiter and clear beach obstacles for troops making amphibious landings. These teams, which served with distinction in both the Atlantic and Pacific theatres of war, became known as underwater demolition teams (UDTs) in Korea. There they took part in the landing at Inchon and engaged in a number of missions involving demolition of bridges and tunnels accessible from the water.

In the early 1960s, as the United States increased its involvement in Vietnam, each military service formed a special warfare unit. In 1962 the Navy SEALs gained formal existence with the commissioning of two SEAL teams, One and Two, which served in the Pacific and Atlantic respectively. In 1983 all UDTs and other naval special-warfare teams were redesignated either as SEAL teams or SEAL delivery vehicle teams. On April 16, 1987, the Naval Special Warfare Command at the Naval Amphibious Base was commissioned to prepare naval special warfare forces through training, doctrine, tactics, and the development of special operations strategy.

Among the most significant activities at Coronado is Basic Underwater Demolition/SEAL (BUD/S) training, a rigorous program that culminates in the notorious “hell week.” During the latter, prospective SEALs are only allowed about four hours’ sleep and must undergo numerous drills that require, among other challenges, heavy

lifting, crawling in wet sand with live ammunition fire overhead, and immersion in ice-cold water.

#### ■ FURTHER READING:

##### BOOKS:

Boehm, Roy, and Charles W. Sasser. *First SEAL*. New York: Pocket Books, 1997.

Bosiljevac, T. J. *SEALs: UDT/SEAL Operations in Vietnam*. New York: Ivy Books, 1991.

Chalker, Dennis C., and Kevin Dockery. *One Perfect Op: An Insider's Account of the Navy SEAL Special Warfare Teams*. New York: Morrow, 2002.

##### ELECTRONIC:

Naval Special Warfare. <<http://www.sealchallenge.navy.mil>> (April 1, 2003).

Navy SEALs.com. <<http://www.navyseals.com>> (April 1, 2003).

##### SEE ALSO

*Delta Force*  
*Special Operations Command, United States*

## Secret Codes.

SEE *Enigma*.



U.S. Navy SEALs found intelligence information, including mine recognition posters, located in an al-Qaeda classroom during a Sensitive Site Exploitation mission in the Zhawar Kili area in eastern Afghanistan in January 2000. AP/WIDE WORLD PHOTOS.

## Secret Service, United States

The United States Secret Service (USSS) has two missions that, while sharply distinguished from one another, are united by the principle of protection. On the one hand, in its more visible role, the service provides protection of the president, vice president, and other dignitaries and their families. On the other hand, USSS's larger mission protects securities, including federal currency and other documents. Established in 1865 as an office under the Department of the Treasury, USSS was transferred in 2003 to the newly created Department of Homeland Security (DHS).

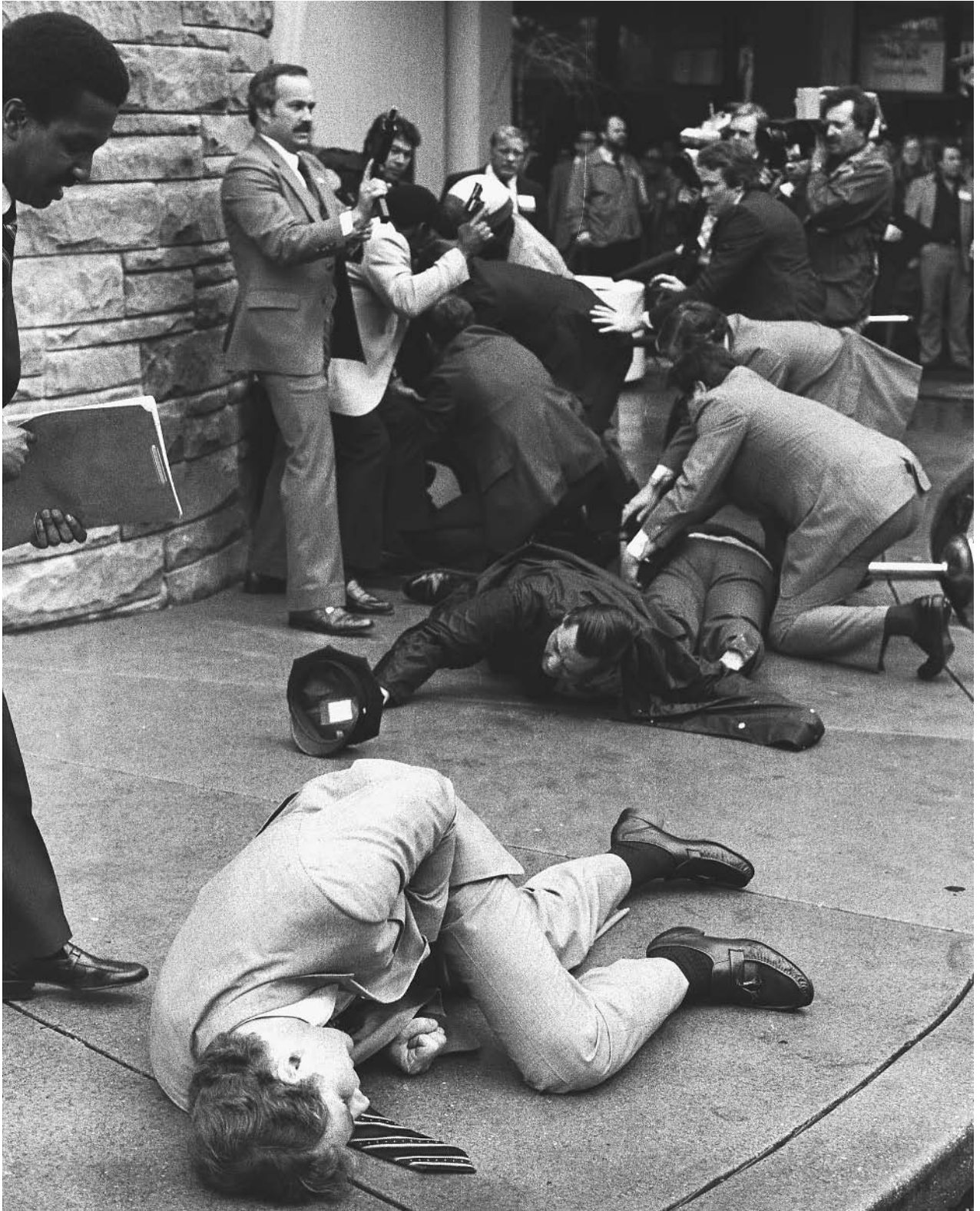
**Early history.** At the time Secret Service was founded, approximately one-third of all currency in circulation was counterfeit. Only in 1877 did Congress pass its first law against the production of counterfeit currency, and even then, the law only encompassed counterfeit coins. By

then, the mission of USSS had broadened, with an order in 1867 charging it with "detecting persons perpetrating frauds against the government"—a mission that soon put the service on the trail of a range of lawbreakers ranging from bootleggers to members of the Ku Klux Klan.

The personal protection mission of USSS had its beginnings in 1894, when it first provided protection to President Grover Cleveland on an informal and part-time basis. Following the assassination of President William McKinley in 1901, Congress officially requested USSS protection for presidents, and in 1902 the Secret Service assumed full-time protective duties for the Chief Executive. At that time, the White House detail numbered just two agents.

**The first half of the twentieth century.** In 1908 President Theodore Roosevelt transferred eight USSS agents to the Department of Justice, where they formed a small contingent that would ultimately become the Federal Bureau of Investigation (FBI). Congress in 1913 authorized USSS to provide permanent protection to U.S. presidents, and in





Secret Service agent Timothy J. McCarthy, foreground, lies wounded outside a Washington hotel after throwing himself in the line of fire of gunshots directed at President Ronald Reagan on March 30, 1981. Washington policeman Timothy Delahanty, center, and Press Secretary James Brady, back, were also wounded along with the president. All those pictured survived their wounds, and McCarthy later returned to duty. AP/WIDE WORLD PHOTOS.

1917 it assigned them to protect presidents' immediate families as well. Also in that year, it became a federal crime to make threats against the president. At the request of President Warren G. Harding, a White House police force was created in 1922, and in 1930 Congress placed this force under USSS direction.

On November 1, 1950, Puerto Rican nationalists attempting to assassinate President Harry S. Truman shot and killed White House police officer Leslie Coffelt. This led Congress to pass legislation formalizing USSS permanent protection for presidents and their immediate families, as well for the president-elect and the vice president. In 1962 Congress again expanded these provisions to include the vice president-elect.

**The modern Secret Service.** After the assassination of President John F. Kennedy on November 22, 1963, awareness of the threat to presidents' lives increased dramatically. The mission of USSS also expanded with regard to the persons under its protection. Congress in late 1963 authorized protection for Mrs. Kennedy and her children for two years, and legislation in 1965 provided protection for a president's spouse, as well as minor children until the age of 16. In June 1968, while on the presidential campaign trail, Kennedy's brother, Senator Robert F. Kennedy, was assassinated. This led to new laws providing Secret Service protection for major presidential and vice presidential candidates and nominees.

The White House Police Force became the Executive Protective Service in 1970, and to its duties was added responsibility for protecting diplomatic missions in Washington, D.C. In the next year, visiting heads of state or government, as well as other official guests, were granted USSS protection. By 1975, the Executive Protective Service was detailed to guard foreign diplomatic missions throughout the United States and its territories. On November 15, 1977, the Executive Protective Service became the Secret Service Uniformed Division, and in October 1986 it absorbed the Treasury Police Force.

Since the Kennedy assassination, only three persons under Secret Service protection have been the target of direct assassination attempts: Alabama governor and third-party presidential candidate George Wallace in 1972, President Gerald Ford in 1975 (twice), and President Ronald Reagan in 1981. All three survived, a circumstance that—particularly in the last instance, when several agents were wounded—owed much to the work of Secret Service.

**From the 1980s onward.** At the same time, USSS continued work in its other field, protecting securities. In 1984 Congress made credit- and debit-card fraud a federal violation, and authorized Secret Service to investigate those crimes, as well as fraud involving identification documents. USSS in 1990 received concurrent jurisdiction with Department of Justice law enforcement personnel to conduct civil and criminal investigations relating to federally

insured financial institutions. In 1994 new legislation provided for the prosecution of persons counterfeiting U.S. currency abroad, assessing them with the same penalties as if they had committed the crime on American soil.

Also in 1994, Congress reduced the lifetime-protection provisions for presidents. All chief executives elected after January 1, 1997, would receive protection only for the first 10 years after leaving office. Under the provisions of the Homeland Security Act of 2002, Secret Service moved to the new DHS.

Though its headquarters are in Washington, D.C., just three blocks from the White House, Secret Service operates more than 120 field offices in all 50 U.S. states. It also has more than a dozen offices in foreign countries. It employs 2,100 special agents, another 1,200 uniformed agents, and some 1,700 support personnel.

**Uniformed and special agents.** Requirements for special agents are somewhat higher than for uniformed officers—for example, a bachelor's degree is a condition of eligibility for the former and not the latter—but standards for both are high, and applicants must pass an extensive series of tests and background checks. Those selected by Secret Service undergo a nine-week training course at the Federal Law Enforcement Training Center in Glynco, Georgia, followed by specialized training. Special-agent candidates take an additional 11-week course at the Secret Service Training Academy in Beltsville, Maryland. Uniformed officers receive varying types of training.

Agents serving in the Uniformed Division provide protection at the White House and a number of other key sites in Washington. They often work with support teams that include countersniper, emergency response, and canine units. Special agents usually spend their first six to eight years in a field office, then are assigned to provide personal protection for three to five years. After this assignment, they may choose a number of paths, continuing in a protective detail, serving in the field, or working in some other capacity.

#### ■ FURTHER READING:

##### BOOKS:

- Department of the Treasury. *Excerpts from the History of the United States Secret Service, 1865–1875*. Washington, D.C.: Department of the Treasury, 1978.
- McCarthy, Dennis V. N. with Philip W. Smith. *Protecting the President: The Inside Story of a Secret Service Agent*. New York: William Morrow, 1985.
- Melanson, Philip H. *The Politics of Protection: The U.S. Secret Service in the Terrorist Age*. New York: Praeger, 1984.
- Motto, Carmine J. *In Crime's Way: A Generation of U.S. Secret Service Adventures*. Boca Raton, FL: CRC Press, 2000.

**ELECTRONIC:**

United States Secret Service. <<http://www.ustreas.gov/uss/>> (February 5, 2003).

**SEE ALSO**

*Counterfeit Currency, Technology and the Manufacture Engraving and Printing, United States Bureau*

---

## Secret Writing

---

Secret writing is any means of written communication whereby a spy conceals the actual written text, whether it is enciphered/encoded or not. Codes and ciphers are sometimes mistakenly placed under the heading of “secret writing,” but this is accurate only if that expression is taken in its most general sense, as writings that are concealed in any way. Whereas codes and ciphers conceal the meaning of a message, secret writing conceals the actual message. Techniques of secret writing include the use of invisible ink and carbon copies. Widely applied from ancient times until the early twentieth century, secret writing has been almost entirely eclipsed by more modern methods of concealing messages, such as microdots.

**An early example of secret writing.** In his venerable *History*, Herodotus described a method of secret writing employed in the Persian Wars. As the Persian emperor Xerxes was preparing to march on the Greek city-states in 480 B.C., a Spartan expatriate name Demaratus learned of the plans and contrived to warn his compatriots. The problem was how to do so in such a way that the Persians themselves would not intercept the message, a challenge for which Demaratus contrived a clever solution.

As Herodotus recorded, Demaratus scraped the wax from a pair of wooden tablets, wrote his message on the wood beneath, then poured hot wax onto the tablets again. Of course the Spartans lacked the advantage of knowing that they were receiving a secret message, but according to Herodotus—who qualified his claim with the caveat “as I understand [it]”—Gorgo, the daughter of a citizen named Cleomenes, received a divine revelation. Thanks to the intervention of the gods, the Spartans realized that they had simply to scrape off the wax and read the message written on the wood beneath it. The Greeks thus began to prepare for the coming invasion, and routed Xerxes’s navies at Salamis.

**Invisible ink.** One form of secret writing known to many children from school projects is invisible ink. This technique uses an acidic citrus juice, of which lemon juice is most often the preferred choice because it dries without

leaving any evidence it has been applied. The juice takes the place of ink, and is applied using a fine stylus (a tool for which an ordinary toothpick will suffice). After the juice dries, the acid remains on the paper, which it weakens, and therefore the message is readily exposed when heat is applied to the paper.

Other liquids for invisible ink include milk, which is mildly acidic, as well as white wine, vinegar, or apple juice. In the past, prisoners of war have used their own sweat, saliva, or even urine, all of which contain acidic secretions that adhere to the paper, weakening it, even after the water in those bodily fluids has evaporated. A slight variation on this technique is the use of a baking soda and water mixture as the invisible ink, and, after drying, applying grape juice concentrate with a paint brush. The acid in the grape juice reacts with the baking soda (a base or alkali in chemical terms), exposing the message.

**Carbon copies.** During the late nineteenth and early twentieth centuries, carbon copies provided a means of secret writing. This method, which was even used by the Central Intelligence Agency (CIA) in its early days, involved a means not unlike the one still used today when signing a credit-card receipt. The back of the receipt is impregnated with graphite, a carbon allotrope (a version of a chemical element distinguished by molecular structure) also used in pencil lead. Therefore, when one signs the front of the receipt, the pressure transfers the graphite to the second page, leaving an impression as though one had written on it in pencil.

The CIA version of this technique involved paper containing a special chemical that would be invisible when transferred to the second sheet. This made it possible to inscribe secret writing on the back of an envelope, which could be mailed to the agent through ordinary channels. Using water or heat, the message could then be developed and read.

**Secret writing today.** The use of secret writing has declined since the middle of the twentieth century for several reasons, most important of which is the sheer volume of data that intelligence services must transmit and process. This has prompted the use of more efficient means for concealing information without having to write it out by hand. One such means was the microdot, or miniaturized photographic image. First used in the mid-1800s, microdots remained popular among intelligence services through the 1960s, their use aided by the development of microdot cameras.

Much more sophisticated is the technique of steganography, the concealment of information within other, apparently innocuous, data in a computer file. Yet, old-fashioned secret writing remained enough of a factor in intelligence that in 1990, the Senate Select Intelligence Committee noted its use by persons conducting espionage against the federal government. In 2002 Russian



An FBI agent is shown using ultraviolet light to read secret writing on a paper from a suspected spy case. ©BETTMANN/CORBIS.

authorities claimed that a Russian Defense Ministry employee had passed information to CIA using invisible ink.

*Dead-Letter Box*  
*Encryption of Data*

#### ■ FURTHER READING:

##### BOOKS:

Gardner, Martin. *Codes, Ciphers, and Secret Writing*. New York: Pocket Books, 1974.

Zim, Herbert Spencer. *Codes and Secret Writing*. New York: W. Morrow, 1948.

##### PERIODICALS:

Ingram, Judith. "Russia Accuses U.S. of Espionage." *Chicago Sun-Times*. (April 11, 2002): 27.

Lardner, George, Jr. "Panel Proposes Tougher Laws against Espionage." *Washington Post*. (May 24, 1990): A16.

##### SEE ALSO

*Cryptology, History*  
*Dead Drop Spike*

## Security Clearance Investigations

■ JUDSON KNIGHT

A security clearance is a limited license or initial general permission to access classified information—that is, any data or material belonging to the federal government that relates to sensitive topics such as military plans or vulnerabilities of security systems. Authorization for a security clearance is far from automatic, but rather requires extensive background checks and investigations. A number of laws, including Executive Order 12968, govern

background investigations and security clearances, but numerous aspects of the topic remain controversial. This is equally so for the private sector, in which background investigations as a precondition for employment are an increasingly familiar fixture of the workplace.

There are three levels of security clearance, corresponding to three levels of classified material: *Confidential*, a term referring to information whose disclosure to unauthorized personnel could reasonably be expected to cause damage to national security; *Secret*, or information whose disclosure to unauthorized personnel could result in serious damage to national security; and *Top Secret*, a term referring to information whose disclosure to unauthorized personnel could reasonably be expected to result in exceptionally grave consequences.

## Background

In addition to the most basic and widely known levels of security clearance, there are numerous other categories, including “need to know” and “compartment.” An individual or agency with a “need to know” has a demonstrable and recognized purpose for accessing specific information. “Compartment,” in the context of security clearances, refers to a group of individuals with a need to know regarding a specific topic.

Each “compartment” has its own code words and access keys for computerized information. For example, the Central Intelligence Agency (CIA) has used specific colors on cover sheets to indicate particular compartments. Such agencies may designate information according both to the level of security clearance and the compartment. Thus, for one compartment of CIA in the 1970s, devoted to aspects of intelligence concerning the Soviet Union, a message might be designated TOP SECRET REDWOOD.

Implementation of the “compartment” concept as such—and, indeed, the concept of the security clearance—goes back to the days just before America’s entry into World War II. At that time, General George Marshall established a list of persons authorized to receive intelligence obtained through the decoding of Japanese diplomatic transmissions. According to Marshall’s “Top List,” access to this compartment, designated MAGIC, would be limited to the president; the secretaries of State, War, and the Navy; and the directors of army and naval intelligence. As Jeffrey T. Richelson noted in *The United States Intelligence Community*, “Among those not on the list was the Commander of United States Naval Forces at Pearl Harbor, Admiral Husband Kimmel.”

During the war, United States and British intelligence developed a number of compartments, and after signing the Brusa Communications Intelligence Agreement in May 1943, the Allies designated high-level shared information as ULTRA, a term that emerged from British intelligence. Usually ULTRA intelligence would carry a second word designating the compartment: for example, ULTRA RABID

referred to traffic analysis intelligence based on intercepted Japanese communications.

In the quarter-century that passed between the beginning of World War II and the height of the Vietnam War, the degree to which the concepts of classified information, compartments, and security clearances matured was nothing short of astounding. Richelson noted this extraordinary development in connection with an interchange during a 1964 Senate Foreign Relations Committee hearing. At the time, the Gulf of Tonkin resolution—which would ultimately give President Lyndon B. Johnson authority to greatly expand the United States presence in Southeast Asia—was under discussion. When committee chairman William Fulbright asked for the source of information on a planned attack by North Vietnamese gun boats against the U.S.S. *Turner Joy* on the night of August 4, Defense Secretary Robert McNamara replied that “We have some problems because the [committee] staff has not been cleared for certain intelligence.”

Senator Frank Lausche expressed bewilderment because, as far as he knew, the committee staff had the highest level of clearance, but Fulbright noted that “he [McNamara] is talking of a special classification of intelligence communications.” When Senator Albert Gore, Sr., asked McNamara to clarify, saying, “I had not heard of this particular super classification,” McNamara replied, “Clearance is above top secret for the particular information on the situation.”

**Sensitive compartmented information.** “Above top secret” might sound like a contradiction in terms, or at least similar to a fantastic invention of a conspiracy buff, but what McNamara referred to was a compartment. As Senate records show, McNamara went on to identify the category of clearance as Special Intelligence, or SI. The latter is in turn part of a category designated Sensitive Compartmented Information (SCI), which the National Foreign Intelligence Board (NFIB) defined in a 1984 report as “data about sophisticated technical systems for collecting intelligence[,] and information collected by those systems.” The systems referred to here would include any and all submarines and ships, ground stations, aircraft, and satellites tasked to the gathering on sensitive information.

Within SCI are several compartments, such as TK or TALENT-KEYHOLE, which concerns data gathered from imaging satellites. SCI also has its own levels of security clearance, ranging from MORAY to SPOKE to UMBRA. To these may be added the more traditional designations mentioned earlier, but even a Confidential document at this high level carries much greater restrictions than an ordinary Top Secret document.

**Executive Order 12968.** One of the most important documents governing access to classified information and the granting of security clearances is Executive Order 12968,

signed by President William J. Clinton on August 4, 1995. Titled “Access to Classified Information,” the order “establishes a uniform Federal personnel security program for employees who will be considered for initial or continued access to classified information.” It provides rules governing access, among which is the requirement that those being considered for such access submit themselves to investigation of financial records. The order calls upon employers to submit the names of employees who might be considered risks for revealing classified information, and to educate employees with regard to their responsibilities to maintain classified information.

At the beginning of Part 2, “Access Eligibility Policy and Procedure,” the order provides for strict limitations on the number of employees in a given office who may be eligible for access to classified information, and notes that such eligibility “shall not be requested or granted solely to permit entry to, or ease of movement within, controlled areas where the employee has no need for access and access to classified information may reasonably be prevented.” Part 3 establishes the standards of eligibility, and Part 4 consists of a single paragraph allowing federal agencies to conduct background investigations on behalf of foreign governments if needed.

Part 5 enumerates the employee’s right to appeal in cases where access is denied. If the denial has occurred because the employee has no justifiable need to know, there is no appeal, but if he or she has been deemed wanting according to the standards established in Section 3.1, then the employee has a right to request an explanation, as well as copies of all documents upon which the denial is based, assuming that access to them is permitted under the Freedom of Information Act.

**Criticisms of 12968.** Despite these provisions, according to the journal *Government Executive*, Executive Order 12968 did not reach as far as some advocated. Federal labor unions and legal experts complain that private sector workers still have more substantial appeal rights “that were unaffected by the executive order.” Writing in the same publication, Richard Lardner described the order as the culmination of efforts to prevent another case like that of Aldrich Ames, the CIA employee arrested in 1994 for passing information to the Soviet Union and later Russia. For his efforts, Ames received a total of \$2 million from Moscow. If the federal government had possessed greater knowledge concerning Ames’s finances, supporters of the new financial disclosure measures maintained, he might have been stopped sooner.

To this end, the order had called for the United States Security Policy Board to develop a financial disclosure form whereby employees could provide information regarding their personal finances. Though the board was given 180 days to develop such a form, Lardner noted, a year and a half had passed without any such document emerging. Furthermore, he argued that there were “plenty of questions as to whether a form makes any sense at all,”

since “Agents willing to betray their country are no more inclined to fill out a financial disclosure form honestly than they are to turn themselves in.”

## Background Investigations

Some 3 million federal employees, as well as about 1.5 million employees of private contracting or consulting firms such as General Dynamics or Boeing, hold security clearances of one kind or another. They receive these only after an extensive series of background checks, which may be as intrusive as they are detailed.

Still, there are gaps in the system. Political parties have often resorted to charges that opponents in government office did not legitimately hold appropriate clearances. These charges reached historical peaks during the 1950s “Red scare” and again during the Clinton administration.

**Procedures for government employees and contractors.** Military personnel and federal employees requesting security clearances are required to fill out Standard Form (SF) 86, “Questionnaire for National Security Positions.” The form, which is rather like an extremely lengthy and detailed version of a job application, then goes to the appropriate investigating authority—for example, the Defense Security Service (DSS) for military personnel. If the clearance requested is Confidential or Secret, there will follow computerized checks with federal and state agencies for information on employment, residences, education, and criminal history. A check of credit history is also conducted.

For Top Secret clearance, in addition to these checks of computerized data, the investigating authority also conducts interviews of personal references given on SF 86, including friends, present and former coworkers and employees, present and former neighbors, and others. Investigators use these references to generate others—i.e., acquaintances mutual to the subject and the reference that the subject may not have listed on the form.

Interviews involve questions about past and present activities, family background, finances, and so on, with an eye toward determining whether the individual has a questionable record involving drugs, alcohol, unexplained foreign travel, criminality, mental imbalance, financial malfeasance, or compromising sexual behavior. Additionally, investigators will check the records of employers, courts, and rental offices, and conduct a one-on-one interview with the subject.

**Non-governmental background investigations.** In the civilian world, background investigations are typically less stringent for a number of reasons. Companies lack both the resources and the power that the federal government has at its disposal, and in any case, it is hard to imagine a situation in which a security breach involving a producer

of game software or soft drinks could impinge on the future of civilization. Nevertheless, non-governmental background investigations can still be quite extensive. Among the devices used by companies to screen employees are drug tests, polygraph tests, medical and physical exams, routine reference checks, and thorough investigations of the individual's criminal history, driving record, financial and credit information, history of civil litigation, and other details. In some cases, investigators may even gather information on the applicant's lifestyle and personal reputation.

Background investigations in the private sector are increasingly big business. Thousands of companies offer their services to investigate virtually every aspect of the job candidate's background, including such sensitive issues as family history. The more thorough private investigators may conduct door-to-door interviews with neighbors, and some even go through the job candidate's trash—which is legal as long as it is on the curb for pickup—to find correspondence, receipts, or other revealing documents or materials.

Naturally, job candidates—especially those disqualified by the results of background checks—have challenged the legality of such activities. Such concerns played a part in the passage of the Fair Credit Reporting Act (FCRA) by Congress in September 1997. The FCRA requires potential employers to obtain written authorization from a job candidate or employee before accessing records from a consumer-reporting agency, and to notify the employee or applicant if any adverse action is taken pursuant to a negative report. According to a study published in *Public Personnel Management*, background and reference checks are potentially so risky, in a legal sense, to employers that many consider alternatives such as personality tests.

#### ■ FURTHER READING:

##### BOOKS:

*The Guide to Background Investigations: A Comprehensive Source Directory for Employee Screening and Background Investigations.* Tulsa, OK: T.I.S.I., 1998.

Newman, Elizabeth L. *Security Clearance Law and Procedure.* Arlington, VA: Dewey Publications, 1998.

Richelson, Jeffrey T. *The United States Intelligence Community*, third edition. Boulder, CO: Westview Press, 1995.

##### PERIODICALS:

"Access Denied." *Government Executive* 29, no. 2 (February 1997): 19.

Bland, Timothy S. "Background Checks: Making a Federal Case." *Journal of Property Management* 64, no. 5 (September/October 2000): 26–31.

Lardner, Richard. "The Need to Know." *Government Executive* 29, no. 2 (February 1997): 16–21.

Terpstra, David E., et al. "The Nature of Litigation Surrounding Five Screening Devices." *Public Personnel Management* 29, no. 1 (spring 2000): 43–54.

#### SEE ALSO

*Ames (Aldrich H.) Espionage Case Classified Information*  
*Clinton Administration (1993–2001), United States National Security Policy*  
*Executive Orders and Presidential Directives*  
*Privacy: Legal and Ethical Issues*

## Security, Infrastructure Protection, and Counterterrorism, United States National Coordinator

The U.S. National Coordinator for Security, Infrastructure Protection, and Counterterrorism is a broadly based office created by Presidential Decision Directive (PDD) 62. Signed by President William J. Clinton on May 22, 1998, PDD 62 authorized the national coordinator to oversee policies and programs in areas ranging from counterterrorism to protection of critical infrastructure (such as computers) to consequence management for weapons of mass destruction.

Known as the Combating Terrorism directive, PDD 62 drew attention to the growing threat of unconventional attacks against the United States. On the same day he issued PDD 62, Clinton signed PDD 63, which created the Critical Infrastructure Assurance Office (CIAO). Though the functions of CIAO and the national coordinator were similar, they reported along quite different chains of command. Whereas CIAO, now part of the Department of Homeland Security (DHS), was then part of the Department of Commerce, the national coordinator reported to the National Security Council (NSC).

Given the fact that the NSC is the president's advisory board on national security affairs, this fact signaled the importance of the new national coordinator. So, too, did Clinton's appointment of Richard A. Clarke, who had served in the State Department of presidents Ronald Reagan and George Bush, and would later receive an appointment as special advisor for cyberspace security under George W. Bush.

Bush kept Clarke, famous for warning of a possible "electronic Pearl Harbor" (that is, a terrorist cyberattack) during the Clinton years, on the NSC. Meanwhile, the appointment of four-star general Wayne A. Downing to take Clarke's place as national coordinator further reinforced the importance of the office. Despite their involvement with the NSC, both the national coordinator and the special advisor for cyberspace security came under the newly created DHS.

## ■ FURTHER READING:

### PERIODICALS:

Verton, Dan. "National IT Protection Plan Update Delayed." *Computerworld*. 35, no. 41 (October 8, 2001): 12.

### ELECTRONIC:

Press Briefing by Richard Clarke, National Coordinator for Security, Infrastructure Protection, and Counterterrorism. Federation of American Scientists. <<http://www.fas.org/irp/news/1998/05/980522-wh3.htm>> (March 26, 2003).

Summary of PDD 62 and PDD 63. Critical Infrastructure Assurance Office. <<http://www.ciao.gov/resource/pdd6263summary.html>> (March 26, 2003).

### SEE ALSO

*Critical Infrastructure*  
*Critical Infrastructure Assurance Office (CIAO), United States*  
*Cyber Security*  
*Homeland Security, United States Department NSC (National Security Council)*  
*United States, Counter-terrorism Policy*

---

## Security Policy Board, United States

---

An advisory committee created by President William J. Clinton in 1994, the Security Policy Board (SPB) reported to the president through the National Security Advisor on matters of security policy. Its short existence was a troubled one, with critics charging that the board's organizational system was too complex and cumbersome. In 2001 the new administration of President George W. Bush abolished the SPB.

On September 16, 1994, Clinton signed Presidential Decision Directive 29 ("Security Policy Coordination"), in which he redesignated the Joint Security Executive Committee, established by the deputy Secretary of Defense and the Director of Central Intelligence (DCI), as the SPB. The latter included the DCI and deputy Secretary of Defense, the vice chairman of the Joint Chiefs of Staff, the deputy Attorney General, and deputy secretaries or undersecretaries of State, Energy, and Commerce. Its job was to consider policy directives and to review and propose legislative initiatives and executive orders relating to U.S. security policy. Additionally, it would coordinate inter-agency agreements and resolve conflicts over these.

In addition to the board itself, there was a Security Policy Advisory Board, a Security Policy Forum, an Overseas Policy Board (formerly the Department of State Overseas Security Policy Group), and their various interagency

working groups. The result was an extremely cumbersome system in which, charged Richard Lardner of *Government Executive*, little was getting done. As of March 1998, the board itself had met only once, in March 1996, and most of its activities took place through various subcommittees and working groups.

The SPB in early 1998 reviewed ties between Commerce Department official John Huang and the Chinese government, and in 1999 severely criticized cost-cutting measures by the Defense Security Service that had resulted in the granting of security clearances to unqualified personnel. On February 13, 2001, Bush dissolved the SPB and other aspects of Clinton's national security structure with National Security Presidential Directive 1, "Organization of the National Security System."

## ■ FURTHER READING:

### PERIODICALS:

Lardner, Richard. "Keeping Secrets." *Government Executive* 30, no. 3 (March 1998): 27–29.

Pound, Edward T. "Security Panel Has Opposed Agency's Cost-Cutting Moves." *USA Today*. (August 20, 1999): 8A.

White, Ben. "Commerce Secretary Unveils New Security Policy." *Washington Post*. (February 11, 1998): A19.

### ELECTRONIC:

Security Policy Board Documents. Federation of American Scientists. <<http://www.fas.org/sgp/spb/>> (April 2, 2003).

### SEE ALSO

*Bush Administration (2001–), United States National Security Policy*  
*Chinese Espionage against the United States*  
*Clinton Administration (1993–2001), United States National Security Policy*  
*Defense Security Service, United States*

## Security Screeners.

SEE *Aviation Security Screeners, United States*.

---

## Seismograph

---

### ■ LAURIE DUNCAN

A seismograph is an instrument that measures and records elastic ground vibrations called seismic waves that are generated by earthquakes and man-made explosions. By recording the arrival of seismic waves at remote seismograph stations, seismologists deduce information about the initial earthquake fault rupture or explosion, and about the physical properties of earth materials between the seismic source and the seismograph. Much of our present



knowledge of Earth's large-scale interior structure came from analysis of seismograph records. Academic, petroleum, and mining geologists use other seismic techniques to study the structure of Earth's outer sedimentary layers, to prospect for petroleum, and to assess mineral ore bodies. Academic seismograph networks designed to detect earthquakes or planned survey explosions also perform double-duty as monitoring systems that detect military explosions that may indicate violations of international weapons bans.

A modern seismograph includes five basic parts: a clock, a sensor called a seismometer that measures intensity of shaking at the instrument's location, a recorder that traces a chart, or seismogram, of the seismic arrivals, an electronic amplifier, and a data recorder that stores the information for later analysis. The clock records precise arrival times of specific seismic waves. The seismometer mechanically measures ground movement by comparing the motion of a support structure that moves with the land surface to a stationary or inertial mass. To measure vertical motion, the inertial mass hangs from the support by a spring; to measure horizontal motion it is suspended on a hinge. The recording device registers seismic vibrations with a pen attached to the inertial mass, and a roll of paper that moves along with the Earth's vibrations. As the paper cylinder oscillates and unwinds at a constant rate, the stationary pen traces a seismogram that shows the amplitude and frequency of shock waves that arrive over time. Today's seismographs often contain electronic sensors and recorders that perform these tasks, but the principles of their operation remain the same.

Scientists have used tools to detect ground motion since the ancient Han Dynasty when Chang Heng, a Chinese astronomer and mathematician, invented the first seismometer in about 132 A.D. Heng's "earthquake weathercock" seismoscope consisted of a pendulum that swung inside a jar surrounded by eight balanced dragon heads, each holding a bronze ball in its moveable jaws. During an earthquake, the pendulum would swing away from the approaching seismic waves, hit one of the dragons, and knock the ball out of its jaws, indicating the direction of the shock waves.

Seismographs have undergone considerable refinement since Heng's time. European scientists of the 1700s and early 1800s developed a series of mercury-filled seismoscopes and pendulum seismometers that attempted to measure the amplitude and frequency of seismic waves, as well as their propagation directions. British seismologist, John Milne, and his colleagues developed the first modern seismographs to observe Japanese earthquakes in the late 1800s. Their seismographs, however, recorded only a limited range of wave sizes and seismic events, the instruments were fairly inaccurate, and they required difficult mechanical calibration. German seismologist, Emil Weichert, invented an inverted, mechanically damped pendulum seismometer that considerably improved the sensitivity and accuracy of Milne's seismometer in 1899. In 1906 Boris Golitsyn, a Soviet physicist and seismologist,

devised an electromagnetic seismograph that operated without mechanical levers, an enhancement of Weichert's instrument. The first modern seismographs in the United States were installed at the University of California at Berkeley and the Lick Observatory at Mount Hamilton, California in 1877. They recorded the 1906 earthquake that devastated San Francisco.

Development of precise seismographs led immediately to discoveries of Earth's interior structure and delineation of its major physical layers: solid inner core, liquid outer core, solid lower mantle, plastic upper mantle, and rigid lithosphere. British seismologist, Richard Oldham (1858–1936) observed that seismic events produce three of different types of waves that travel away from an earthquake focus at different speeds, and named them surface waves, P (Primary or Pressure) waves, and S (Secondary or Shear) waves. Oldham and Weichert confirmed the existence of Earth's core in 1906 by comparing the paths of P waves and S waves through the planet's interior. Yugoslavian seismologist and meteorologist, Andrija Mohorovicic (1857–1936) used seismograph records to define the Mohorovicic seismic discontinuity, or Moho, at the boundary of the iron-rich mantle and the silica-rich crust in 1909. The Danish seismologist, Inge Lehmann, discovered of the boundary between Earth's liquid outer and solid inner core in 1914.

Today, seismologists continue to use seismograph records to make discoveries about Earth's interior structure, to prospect for petroleum and minerals, and to monitor large military explosions. The Incorporated Research Institutions for Seismology (IRIS) consortium, for example, operates the Global Seismograph Network (GSN) of about 120 permanent seismographs that continuously record seismic events around the planet and transmit their data to a publicly available data base. The GSN, like its precursor, the World-Wide Seismograph Network (WWSN), detects all but the smallest earthquakes worldwide, as well as seismic waves emitted by nuclear explosions and detonations of large conventional weapons. The academic members of IRIS provide data and analyses in support of the international Comprehensive Test Ban Treaty (CTBT) that seeks to monitor international weapons tests, and identify treaty violations.

#### ■ FURTHER READING:

##### BOOKS:

- Fowler, C. M. R. *The Solid Earth*. Cambridge: University Press, 1990.
- Press, Frank and Raymond Siever. *Understanding Earth*. New York: W.H. Freeman and Company, 2000.

##### ELECTRONIC:

- Incorporated Research Institutions for Seismology. "Welcome to the IRIS Homepage." December 3, 2001. <<http://www.iris.edu>>(December 28, 2002).

United States Geological Survey Earthquake Hazards Program. "Seismology." National Earthquake Information Center and World Data Center for Seismology, Denver. April 5, 2001. <<http://neic.usgs.gov/neis/seismology/>> (December 28, 2002).

#### SEE ALSO

*Seismology for Monitoring Explosions*

## Seismology for Monitoring Explosions

■ WILLIAM C. HANEBERG

Seismology has been an important tool for the remote detection of large explosions, especially underground nuclear tests, for many years and is expected to play an important role in Comprehensive Test Ban Treaty verification. The treaty was signed by President Clinton and other world leaders in 1996, and was subsequently ratified by the United States Congress in 1999.

The Limited Test Ban Treaty of 1963 curtailed nuclear testing in the atmosphere, outer space, and under water, leaving underground testing as the only option. The Threshold Test Ban Treaty, signed in 1974, further banned nuclear explosions larger than 150 kilotons. For that reason, Threshold Test Ban Treaty verification concentrated on estimation of explosion size. Explosions large enough to exceed the 150-kiloton limit create earthquakes that are easily detected by seismometers thousands of kilometers away.

Because the Comprehensive Test Ban Treaty forbids all nuclear testing, seismologists have redirected their attention toward the detection of nuclear explosions, regardless of size. This is a difficult task because each day there are hundreds of naturally occurring earthquakes and large non-nuclear industrial explosions associated, for example, with mining and building demolitions. It is generally possible, however, to distinguish earthquakes caused by explosions from naturally occurring earthquakes along faults. In comparison to naturally occurring earthquakes, earthquakes triggered by explosions are very shallow. Explosions occur in small spaces and, because an explosion causes the rock around it to dilate, produce strong compressional body waves that travel through the Earth. Earthquakes along faults, in contrast, are caused by slip distributed over large areas and tend to produce much larger surface waves that travel along Earth's surface. Each of these produces distinctly different seismograms and ratios of long- to short-period seismic waves. The size of an explosion can be estimated from the magnitude of the earthquake it produces. Current efforts are aimed at the identification of nuclear explosions in the 0.001 to 0.01

kiloton range, which produce earthquakes of magnitude 2 to 3.

One of the most significant events since the signing of the Comprehensive Test Ban Treaty was a series of nuclear tests conducted by India and Pakistan in May 1998. India, which was one of only three countries to oppose the treaty, conducted three nuclear tests in the northwestern part of the country. Neighboring Pakistan, which supported the treaty, but refused to sign it as long as it was opposed by India, conducted five nuclear tests in response. The tests produced earthquakes with magnitudes between 4.8 and 5.2, one of which was preceded by a naturally occurring magnitude 6.9 earthquake in Afghanistan. Seismologists have concluded that both India and Pakistan probably exaggerated the size of the tests in order to present more powerful images to each other.

The use of seismology to detect remote explosions is not limited to nuclear test monitoring. It can also be used to learn about large explosions due to other causes, especially in foreign countries or inaccessible areas. Seismologists using publicly available information, for example, were able to determine that two separate explosions occurred when the Russian submarine *Kursk* sank in August 2000. A small explosion was followed about two minutes later by a second explosion that released about 16 times as much energy as the first and produced a magnitude 4.2 earthquake that was recorded as far as 5000 km away. It was further determined that the energy released in the second explosion was equivalent to that which would have been released by 2000 to 4000 kg (about 2 to 4 kilotons) of TNT. The depth of the second explosion was estimated from a bubble pulse produced during the explosion, which was caused when a bubble of hot gas oscillates while rising quickly through the water. The calculated depth of 100 m is about the same as the seafloor depth at the location of the *Kursk* accident, so the second explosion probably occurred when the sinking submarine struck the seafloor. More than 150 earthquakes with magnitudes of 1.4 to 1.6 occurred in the months after the sinking. They were probably caused by depth charges that were detonated by the Russian navy to discourage foreign submarines from visiting the wreckage. Similar studies have shed light on incidents such as the 1995 attack on the Murrah Federal Building in Oklahoma City; the 1998 truck-bombing of the American Embassy in Nairobi, Kenya; and the September 11, 2001 terrorist attacks on the World Trade Center and Pentagon.

#### ■ FURTHER READING:

##### PERIODICALS:

Sykes, L.R. "Four Decades of Progress in Seismic Identification Help Verify the CTBT." *Eos, Transactions, American Geophysical Union* vol. 83, no. 44 (October 29, 2002): 497, 500.

Wallace, T.C. "The May 1998 India and Pakistan Nuclear Tests." *Seismic Research Letters* vol. 69 (1998): 386–93.

## ELECTRONIC:

Koper, Keith. "Seismology and Nuclear Explosions." August 21, 2002. St. Louis University. <<http://mnw.eas.slu.edu/People/KKoper/EASA-130/gt>>(6 December 2002).

United States Department of Energy. "Nuclear Explosion Monitoring Research & Engineering Home Page." December 5, 2002. <<http://www.nemre.nn.doe.gov/nemre/>>(5 December 2002).

Wallace, Terry C. "Did Iraq Test a Nuclear Weapon in 1989?" University of Arizona. <<http://www.geo.arizona.edu/geophysics/faculty/wallace/IRAQ/>>(5 December 2002).

———. "Forensic Seismology and the Sinking of the Kursk." University of Arizona. <<http://www.geo.arizona.edu/geophysics/faculty/wallace/RUSSIANSUB/>>(5 December 2002).

## SEE ALSO

*Clinton Administration (1993–2001), United States National Security Policy*  
*DOE (United States Department of Energy)*  
*Nonproliferation and National Security, United States Nuclear Detection Devices*  
*Nuclear Weapons*  
*Seismograph*  
*Seismology for Monitoring Explosions*  
*Weapons of Mass Destruction, Detection*

## Senate Select Committee on Intelligence, United States

Established in the wake of congressional investigations regarding activities of United States intelligence services in the 1970s, the Senate Select Committee on Intelligence (SSCI) is, along with the House Permanent Select Committee on Intelligence, the principal means by which Congress oversees the intelligence community. In addition to reviewing, studying, and reporting on intelligence activities and programs, the SSCI is responsible for submitting to the Senate appropriate proposals for legislation.

The SSCI was created by Senate Resolution 400 in 1976, the same year that the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, chaired by Frank Church (D-ID), completed its investigations of U.S. intelligence activities. Whereas the relationship of the Church Committee to the intelligence community was largely adversarial, the SSCI has developed as an entity that, while maintaining scrutiny of intelligence activities, also makes recommendations to increase the effectiveness of U.S. intelligence.

Each year, the SSCI undertakes a review of the intelligence budget submitted by the president, and prepares legislation authorizing appropriations for civilian and military agencies within the intelligence community. The SSCI

also makes recommendations to the Senate Armed Services Committee regarding authorizations for intelligence activities of the military services.

During the late twentieth and early twenty-first centuries, areas of focus for the SSCI included modernization of the U.S. signals intelligence system and improving the implementation of intelligence obtained from satellites and other collection platforms. Particular areas of concern under the administration of President William J. Clinton included satellite and missile technology transfers to the People's Republic of China and Chinese efforts to influence U.S. policy.

## ■ FURTHER READING:

## BOOKS:

*Legislative Oversight of Intelligence Activities: The U.S. Experience: A Report.* Washington, D.C.: U.S. Government Printing Office, 1994.

Smist, Frank John. *Congress Oversees the United States Intelligence Community, 1947–1994.* Knoxville: University of Tennessee Press, 1994.

Wittkopf, Eugene R., and James M. McCormick. *The Domestic Sources of American Foreign Policy: Insights and Evidence.* Lanham, MD: Rowman and Littlefield Publishers, 1999.

## ELECTRONIC:

Intelligence Laws and Regulations. Federation of American Scientists. <<http://www.fas.org/irp/offdocs/laws.htm>> (March 26, 2003).

Intelligence Oversight. <[http://intellinet.muskingum.edu/oversight\\_folder/oversighttoc.html](http://intellinet.muskingum.edu/oversight_folder/oversighttoc.html)> (March 26, 2003).

U.S. Senate Select Committee on Intelligence. <<http://intelligence.senate.gov/>> (April 2, 2003).

## SEE ALSO

*Bush Administration (2001–), United States National Security Policy*  
*Church Committee*  
*CIA, Legal Restriction*  
*Clinton Administration (1993–2001), United States National Security Policy*  
*Intelligence Authorization Acts, United States Congress*  
*Intelligence, United States Congressional Oversight*

## Sendero Luminoso (Shining Path, or SL)

Former university professor Abimael Guzman formed Sendero Luminoso (Shining Path, or SL) in the late 1960s,

and his teachings created the foundation of SL's militant Maoist doctrine. In the 1980s, SL became one of the most ruthless terrorist groups in the Western Hemisphere; approximately 30,000 persons have died since Shining Path took up arms in 1980. Shining Path's stated goal is to destroy existing Peruvian institutions and replace them with a communist peasant revolutionary regime. It also opposes any influence by foreign governments, as well as by other Latin American guerrilla groups, especially the Tupac Amaru Revolutionary Movement (MRTA).

In 2001 the Peruvian National Police thwarted an SL attack against "an American objective," possibly the U.S. Embassy, when they arrested two Lima SL cell members. Additionally, government authorities continued to arrest and prosecute active SL members, including Ruller Mazombite (a.k.a. "Camarada Cayo"), chief of the protection team of SL leader Macario Ala, (a.k.a. "Artemio"), and Evorcio Ascencios (a.k.a. "Camarada Canale"), logistics chief of the Huallaga Regional Committee. Recent counterterrorist operations targeted pockets of terrorist activity in the Upper Huallaga River Valley and the Apurimac/Ene River Valley, where SL columns continued to conduct periodic attacks.

**Organization Activities.** The Shining Path has conducted indiscriminate bombing campaigns and selective assassinations. Shining Path adherents detonated explosives at diplomatic missions of several countries in Peru in 1990, including an attempt to car bomb the U.S. Embassy. Peruvian authorities continue operations against the Shining Path groups in the countryside, where Shining Path conducts periodic raids on villages.

Actual Shining Path membership is unknown, but is estimated by U.S. government experts to be about 200 armed militants. SL's strength has been vastly diminished by arrests and desertions. The Shining Path operates in Peru, with most activity in rural areas.

## ■ FURTHER READING:

### ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001, Annual Report: On the record briefing. May 21, 2002 <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

### SEE ALSO

*Terrorism, Philosophical and Ideological Origins  
Terrorist and Para-State Organizations  
Terrorist Organization List, United States  
Terrorist Organizations, Freezing of Assets*

## SENTRI (Secure Electronic Network for Travelers' Rapid Inspection)

The SENTRI (Secure Electronic Network for Travelers' Rapid Inspection) is a component of the Port Passenger Accelerated Service System (PORTPASS) in use at selected border crossings (e.g., crossings at the U.S. and Mexico border in California and Texas) to facilitate quick passage through entry inspection checkpoints. SENTRI and other expedited U.S. national entry systems are designed to identify pre-approved low-risk international travelers using a combination of biometric measurements and encodable data. Automated entry systems are designed to allow inspectors additional time to focus on high-risk entrants.

SENTRI screens program participants and their vehicles against information formerly maintained in former INS and U.S. Customs Service databases. On March 1, 2003, custody of the database was assumed by the Department of Homeland Security (DHS).

SENTRI applicants are fingerprinted, and agents conduct background investigations to verify immigration status and assure the applicant has no prior criminal record. Prior to DHS reorganization, U.S. custom agents were responsible for conducting screening interviews and for conducting preliminary vehicle inspections.

SENTRI features dedicated commuter lanes at entry points. SENTRI systems utilize a combination of technologies to verify the identity of individuals in vehicles. SENTRI's dedicated commuter lanes also use a radio frequency tags affixed to the vehicle to allow moving identification of the vehicle.

When an approved SENTRI participant passes through the SENTRI system, digital license plate readers and camera scans allow inspectors to validate both the identity of the vehicle and the identity of the occupants of the vehicle against digitized photographs of approved participants in the SENTRI database and other law enforcement databases.

Initially, a system of barricades funnels traffic to an automated inspection zone where the SENTRI Automatic Vehicle (AVI) system, consisting of an in-ground inductive loop and a free-standing light curtain, scans the vehicle. The system then interrogates an RF transmitter located on the vehicle. The ensuing transmission of data primes subsequent systems for analysis and comparison of physical data and data stored in the SENTRI database. Data comparisons are also made between data encoded on a magnetic stripe on the program participant's PORTPASS identification card. Either in person or via camera, inspectors also visually compare prospective entrants against the data maintained in the SENTRI database. Lacking a positive identification, some combination of electric gates,

tire shredders, and traffic restriction barriers prevent physical passage through the entry checkpoint.

As with other automated entry systems, SENTRI utilizes a "one-to-one" search protocol to verify identity. Instead of comparing input data across a broad database, an identification number allows direct comparison with the data on file for a particular PORTPASS identification number. Biometric measurements, including fingerprints are also associated with the PORTPASS SENTRI identification number should further identity interrogation be required. Unlike fingerprint search protocols used by the FBI, the entry search protocols are, as of March 2003, unable to take biometrics and conduct a broad search to identify a subject's identity.

As of March 1, 2003, the newly created DHS absorbed the former Immigration and Naturalization Service (INS). All INS border patrol agents and investigators—along with agents from the U.S. Customs Service and Transportation Security Administration—were placed under the direction of the DHS Directorate of Border and Transportation Security (BTS). Responsibility for U.S. border security and the enforcement of immigration laws was transferred to BTS.

BTS is also scheduled to incorporate the United States Customs Service (previously part of the Department of Treasury).

Former INS immigration service functions are scheduled to be placed under the direction of the DHS Bureau of Citizenship and Immigration Services. Under the reorganization the INS formally ceases to exist on the date the last of its functions are transferred.

Although the description of the technologies involved in the SENTRI entry security program remained stable, in an effort to facilitate border security BTS plans envision higher levels of coordination between formerly separate agencies and databases. As of April 2003, the specific coordination and future of the SENTRI program was uncertain with regard to name changes, program administration, and policy changes.

## ■ FURTHER READING:

### ELECTRONIC:

Department of Homeland Security. April 2, 2003. <<http://www.dhs.gov/dhspublic/index.jsp>> (April 11, 2003).

Department of Homeland Security. Secure Electronic Network for Travelers Rapid Inspection (SENTRI). March 26, 2003. <<http://www.immigration.gov/graphics/shared/lawenfor/bmgmt/inspect/sentri.htm>> (April 9, 2003).

United States Department of Homeland Security. Immigration Information, INSPASS. March 4, 2003. <<http://www.immigration.gov/graphics/shared/howdoi/inspass.htm>> (April 9, 2003).

United States Department of Homeland Security. Bureau of Citizenship and Immigration Services, PORTPASS.

March 11, 2003. <<http://www.immigration.gov/graphics/howdoi/portpass.htm>> (April 9, 2003).

## SEE ALSO

*APIS (Advance Passenger Information System)*

*IBIS (Interagency Border Inspection System)*

*IDENT (Automated Biometric Identification System)*

*INSPASS (Immigration and Naturalization Service Passenger Accelerated Service System)*

*NAILS (National Automated Immigration Lookout System)*

*PORTPASS (Port Passenger Accelerated Service System)*

# September 11 Terrorist Attacks on the United States

■ K. LEE LERNER

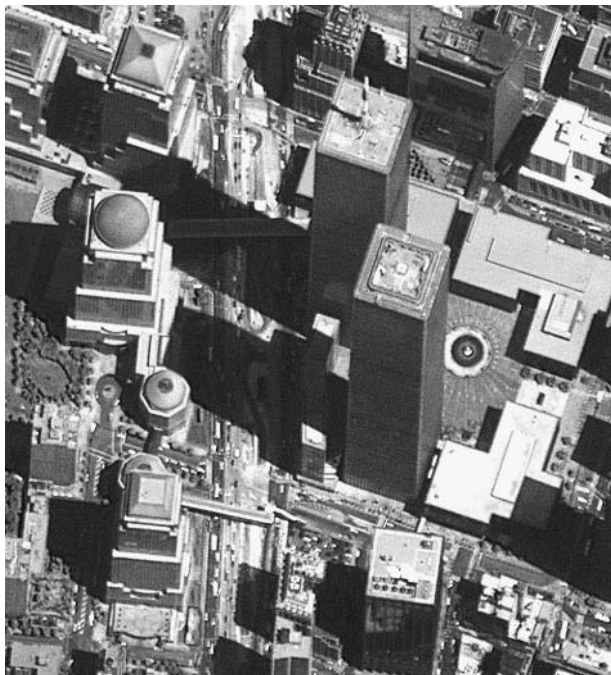
On September 11, 2001, 19 al-Qaeda-trained terrorists hijacked four U.S. commercial airliners. The hijackers crashed two of the jets into the World Trade Center towers in New York City and crashed the third jet into the Pentagon outside Washington, D.C. Passengers and crew battled the hijackers for control of the fourth jet, and it crashed into a field near Shanksville, Pennsylvania, short of reaching the hijackers' intended target in Washington, D.C.

The attacks caused the subsequent collapse of the World Trade Center twin towers, damaged the Pentagon, and killed approximately 3,000 people. Included in the death toll were hundreds of firefighters and rescue personnel who responded to the crashes at the World Trade Center site and who were in the process of rescuing those inside when the buildings collapsed.

Al-Qaeda (also known as al-Qaida), and its leader, Osama bin Laden (also spelled Usama Bin Ladin or Osama bin Ladin), subsequently claimed responsibility for the attacks. Al-Qaeda—operating out of Afghanistan under the protection of the fundamentalist Taliban regime—and allied Islamic extremist groups had publicly vowed a terrorist war against the U.S. and Western interests in an effort to establish pro-Islamist governments and fundamentalist Islamist social order throughout the world. Al-Qaeda also directed the 2000 attack on the USS *Cole* near the port of Aden, Yemen, and claimed responsibility for the bombings of U.S. embassies in Africa.

The September 11, 2001 attacks were the most deadly international terrorist attack in history and the largest attack on United States territory since the Japanese attack on Pearl Harbor on December 7, 1941.

According to investigators and transcripts of cellular phone calls made by passengers aboard several of the



Satellite views of lower Manhattan before the September 11, 2001, terrorist attacks. SPACE IMAGING.



Satellite views of lower Manhattan after the September 11, 2001, terrorist attacks. SPACE IMAGING.

hijacked planes, the hijackers used box cutter knives as weapons to overpower or kill crew and resisting passengers. The aircraft, all destined for long flights and heavy with jet fuel, exploded as powerful bombs upon impact.

**The hijacking of American Airlines flight 11.** The terrorist action began when five terrorists hijacked American Airlines flight 11, a Boeing 767 aircraft carrying 92 people that departed Boston bound for Los Angeles at 8:00 A.M. The FBI subsequently identified the hijackers as Satam M.A. al-Suqami (most hijackers had multiple aliases), Waleed M. al-Shehri, Wail M. al-Shehri; Mohamed Atta, and Abdulaziz Alomari. The hijackers flew American Airlines flight 11 into the North Tower of the World Trade Center in New York City at 8:46 A.M.

**The hijacking of United Airlines flight 175.** Five terrorists hijacked United Airlines flight 175, a Boeing 767 aircraft that departed Boston for Los Angeles at 8:14 A.M. with 65 people on board. The FBI subsequently identified the hijackers as Marwan al-Shehhi, Fayez Rashid Ahmed Hassan al-Qadi Banihammad, Ahmed Alghamdi, and Mohand al-Shehri. The hijackers piloted United Airlines flight 175 into the South Tower of the World Trade Center at 9:03 A.M., 17 minutes after the crash of American Airlines flight 11 into the North Tower.

**The hijacking of American Airlines flight 77.** Five terrorists hijacked American Airlines flight 77, a Boeing 757 carrying

64 people that took off from Washington Dulles Airport bound for Los Angeles at 8:21 A.M. The FBI subsequently identified the hijackers as Khalid Almihdhar, Majed Moqed, Nawaf Alhazmi, Salem Alhazmi, and Hani Hanjour. The terrorists crashed the plane into the Pentagon at 9:43 A.M. The crash into the Pentagon—exactly 60 years to the day after construction began on the building—killed more than one hundred personnel working in the building's outer rings, as well as the people aboard the aircraft. The portion of the Pentagon damaged by the crash had recently been strengthened and remodeled to heighten physical security, and Pentagon officials credit those measures with saving many lives.

**The hijacking of United Airlines flight 93.** Four terrorists hijacked United Airlines flight 93, a Boeing 757 carrying 44 people that took off from Newark bound for San Francisco at 8:41 A.M. The FBI subsequently identified the hijackers as Saeed Alghamdi, Ahmed Ibrahim A. Al Haznawi, Ahmed Alnami, and Ziad Samir Jarrah. Passengers, made aware of the hijackers' intentions during cell phone calls to family and authorities, attempted to overpower the hijackers. Minutes prior to the crash of the aircraft, a passenger on the flight used his cell phone to call an emergency operator in Pennsylvania to report that the plane had been hijacked and that passengers and crewmembers were planning to attempt to retake the plane. At the cost of their own lives, the passengers and crew thwarted the hijackers' plans to crash the plane into a Washington area target. At 10:07 A.M. the aircraft crashed into a field southeast of



The Pentagon on September 12, 2001, as seen in a satellite image with damage visible from the previous day's terrorist attack in the upper right. SPACE IMAGING.

Pittsburgh, Pennsylvania, killing everyone on board. Intelligence developed from subsequently captured al-Qaeda terrorists indicated that the terrorists planned to crash the plane into either the U.S. Capitol or White House.

As of May, 2003, the NTSB (National Transportation Safety Board) continues to investigate the actual September 11, 2001 airline crashes associated with the terrorist attacks.

**National emergency responses.** At approximately 9:30 A.M., U.S. President George W. Bush, who had been visiting a Florida elementary school, spoke briefly to reporters as the Secret Service whisked him away to the security of *Air Force One*. Bush, now aware that the crashes into the World Trade Center were deliberate, but speaking ten minutes before the crash into the Pentagon, pledged that United States would find and punish the parties responsible for crashing the hijacked aircraft into the World Trade Center towers.

Minutes later, the crash into the Pentagon put official Washington into a heightened state of alert and lockdown. The U.S. Capitol, White House, State Department, Justice Department, and World Bank were evacuated.

For the first time in aviation history the Federal Aviation Administration banned all aircraft flights in United States airspace. In a largely unheralded effort, by 12:15 P.M. the airspace over the continental United States was cleared of more than 4,500 commercial and private aircraft. Pilot and air traffic controllers managed to safely land all planes, many far from their intended destinations.

The FAA ban did not reopen airspace until September 13, 2001.

During a tense afternoon and for days afterwards, U.S. military deployed anti-aircraft and anti-missile batteries around New York and Washington. Five destroyers and two aircraft carriers deployed to sea from the Naval Air Station at Norfolk to monitor and protect the U.S. East Coast. Fighter and surveillance aircraft patrolled the skies over major U.S. cities.

**The collapse of the World Trade Center towers.** On a typical workday, an estimated 50,000 people worked in the World Trade Center complex of six buildings. Built in the 1970s, the complex included 110 -story twin towers. Prior to September 11, 2001, the World Trade Center contained offices for more than 400 companies from more than 25 countries and hosted more than 125,000 visitors each day.

Although the full details are not yet known, forensic analysis indicated that the high temperatures of the jet fuel burning in the World Trade Center towers weakened critical supporting beams. As emergency personnel raced into the building to complete the evacuation of those stranded by the fire and to begin the long climb to attack the fire on the upper floors, at 10:05 A.M. the South tower of the World Trade Center suddenly collapsed as the upper floors pancaked into lower floors. The tower collapsed nearly vertically into the deep subfloors and subterranean ground transit station. Above ground, a billowing cloud of pulverized concrete and dust blew through several blocks of lower Manhattan. A mushroom-like plume replaced the South tower in the New York skyline. The slowly clearing air revealed an above ground pile of twisted steel and pulverized wreckage. At 10:28 A.M., the North tower of the World Trade Center collapsed with all the violence of its twin. A third World Trade Center building (the 47-story "Building 7"), damaged by the falling towers, collapsed approximately seven hours later.

Rescue efforts started immediately as surviving police, firefighters, engineers, construction workers, and other arriving emergency personnel began a determined search for colleagues and civilian survivors. Although intense rescue efforts continued for more than a week, the tremendous force of the collapsing buildings spared few of those trapped inside. The tremendous volume of falling material compacted into a tight and dense mass, providing few spaces that held the possibility of finding survivors. Death for thousands had been swift, and beyond a handful of survivors found in the first hours, no one survived the full fury of the collapse. Despite a 24-hour operation throughout the winter by large and dedicated crews, a full excavation of the site and forensic determinations of human remains would take more than half a year.

**The U.S. moves to full alert.** Initially unaware of the extent or origin of the attack, following the attack on the Pentagon, the U.S. military was placed on full nuclear alert. In

accordance with national security protocols and continuity of government measures, President Bush was taken by *Air Force One* to Barksdale Air Force Base in Louisiana and then to the headquarters of the U.S. Strategic Air Command at Offutt Air Force Base in Nebraska. The Secret Service did not determine that it was safe for the president to return to Washington for several hours, but President Bush reportedly asked to return to the White House as soon as possible. Arriving at 7:00 P.M., within an hour and a half the president addressed the nation and vowed to find and punish the perpetrators of the terrorist attacks.

Bush subsequently activated 50,000 National Guard and Reserve members to help with rescue efforts and security.

FEMA, EPA, and scores of federal law enforcement and investigative agencies sent disaster management teams and technical aid to the crash sites.

The FBI dedicated 7,000 of its 11,000 Special Agents and thousands of FBI support personnel to the PENTTBOM investigation. "PENTTBOM" is short for Pentagon, Twin Towers Bombing.

Investigators subsequently determined that the hijackers had been in the United States for periods ranging from a week to several years. Most entered with student or tourist visas and some of those visas had expired prior to September 11. One hijacker admitted to the U.S. to study English attended the school that admitted him. A GAO report issued in 2002 revealed that 13 of the hijackers involved in the September 11 incidents had not been interviewed by U.S. consular officials prior to the granting of visas.

Hijackers Alshehri, Atta, Alomari, Shehhi, and Jarrah were all known to have pilot training. Some of the hijackers had taken pilot training in limited aspects of flight, including training in commercial jet simulators for take-off and flight, but not for landings. Mohamed Atta was identified as the terrorist group leader.

The majority of the hijackers were Saudi nationals, Atta was an Egyptian national.

In 2002 Zacarias Moussaoui, a 34-year-old French citizen of Moroccan origin, was charged with six counts of conspiracy and faced a possible death sentence for alleged involvement in the attacks on New York and Washington. Moussaoui, indicated as the "20th hijacker" by U.S. justice officials, was unable to participate in the mission because he was already under arrest. Moussaoui has denied involvement in the attacks, but admitted to being a member of the al-Qaeda network.

The circumstances surrounding Moussaoui's arrest also sparked controversy and calls for reform with the FBI. An FBI internal investigation following the September 11 terrorist attacks revealed that Special Agent Colleen Rowley of the Minneapolis office had requested a warrant to conduct electronic surveillance and a computer search against Moussaoui well before the September 11 attacks.

Rowley was suspicious of Moussaoui's activities at a local flight school that reported that Moussaoui told instructors that he was only interested in take-off and in-flight operations, but did not care to learn how to land a plane. Moussaoui was arrested for immigration violations prior to the September 11 terrorist attacks, but supervisors denied Rowley's request for a search warrant. Subsequent examination of Moussaoui's computer records revealed phone numbers used by other September 11th hijackers.

**International reactions.** Citizens of 90 countries perished in the terrorist attacks. There was an outpouring of sympathy from much of the world. French President Jacques Chirac was the first foreign leader to visit the World Trade Center site to express French solidarity with the American people. *Le Monde*, the leading French newspaper, ran a sympathetic headline proclaiming solidarity with Americans in their mourning. The United Kingdom lost 67 citizens in the attack, and U.K. Prime Minister Tony Blair pledged full support for the forming U.S. war on terrorism.

Not all reactions were positive; in some Arab cities there were jubilant street celebrations. Unfounded rumors and disinformation swept the Internet that Jewish citizens had mysteriously been forewarned of the attack. In fact, Israeli citizens were among the doomed hijacked passengers and other Israelis died in the World Trade Center collapses. A best-selling book in France speciously claimed that the crash into the Pentagon was a hoax.

In the wake of the September 11 attacks, the Bush administration, with the majority of Congress supporting, effectively declared war on terrorism. Casting aside diplomatic formalities, Bush reverted to the language and ethics of the American frontier when he asserted that bin Laden was wanted "dead or alive" and that, "if he can not be brought to American justice, American justice will find him."

The Old West analogies confounded many of America's European allies, but revealed a deep and fundamental shift in American foreign policy. The emerging Bush doctrine asserted that in the coming war on terrorism, "states were either for us or against us" and that "states that harbor or aid terrorists are as guilty as the terrorists themselves."

Attorney General John Ashcroft and FBI Director Robert S. Mueller, III restructured the Federal Bureau of Investigation's efforts toward counterterrorism. Congress passed and Bush signed into law the Patriot Act into law, giving the FBI and CIA broader investigatory powers and allowing them to share confidential information about suspected terrorists.

With Congressional support, Administration officials created an Office of Homeland Security and put into motion the subsequent creation of the Department of Homeland Security.



The September 11 attacks changed many aspects of American life and governmental policies. Almost every government agency reacted to the attack, changing or implementing emergency protocols and policies directed toward increased security. For example, the FAA enacted tougher airport security measures, required background checks for all airport employees with access to secure areas, and published new rules prohibiting passengers from carrying-on knives and other potential weapons. Airline and airport security reform was a key aspect of international anti-terrorist efforts. The U.S. dramatically increased air marshal protections, swelling the police force from approximately 35 officers pre-September 11 to more than a thousand officers. In addition, prior to departure of every international flight bound for the United States, APIS (Advance Passenger Information System) data is now checked against the Interagency IBIS (Interagency Border Inspection System) database. The Computer Assisted Passenger Prescreening System (CAPPS), used selectively used before September 11, came into regular use at American airports. Security screeners were placed under the control of the newly created Transportation Security Administration (TSA) and airports were required to use explosive-detection devices in the inspection of passengers and baggage.

Intelligence analysts asserted that a lack of human intelligence and over-reliance on technological spying contributed to failures to develop information that might have specifically predicted the attacks. In the aftermath of the attacks, the CIA and other agencies placed a renewed emphasis on the gathering of intelligence from human sources.

#### ■ FURTHER READING:

##### BOOKS:

- Halberstam, David. *New York September 11*. New York: PowerHouse Books, 2001.
- Langewiesche, William. *American Ground: Unbuilding the World Trade Center*. North Point Press, 2002.
- One Nation: America Remembers September 11, 2001*. Boston: Little, Brown, 2001.

##### PERIODICALS:

- "Black September 11." *Air Force Magazine* 95, no. 9 (September 2002): 46–53.
- "Responses to ASR's Survey on Aviation Security Post-Sept. 11." *Airport Security Report* 9, no. 19 (September 11, 2002): 1.
- Thomas, Evan. "The Road to September 11." *Newsweek*. 138, no. 14 (October 1, 2001): 38–49.

##### ELECTRONIC:

- "Nuclear Security—Before and after September 11." U.S. Nuclear Regulatory Commission. September 23, 2002. <<http://www.nrc.gov/what-we-do/safeguards/response-911.html>> (December 11, 2002).

Federal Aviation Administration. "Fact Sheet: Chronology of Events on September 11, 2001" <<http://www1.faa.gov/index.cfm/apa/1064/320D8B51-A894-4E4F-AFA3B5A9A475A46D>> (May 25, 2003).

U.S. Department of State. International Information Programs. "September 11, 2001. Basic Facts" August 15, 2002. <<http://usinfo.state.gov/topical/pol/terror/020815basic.htm>> (May 25, 2003).

U.S. Department of State. "Patterns of Global Terrorism, 2001." <<http://www.state.gov/s/ct/rls/pgtrpt/2001/html/10235.htm>> (May 25, 2003).

The White House. September 11, 2001. "Statement by the President in His Address to the Nation" <<http://www.whitehouse.gov/news/releases/2001/09/20010911-16.html#>> (May 25, 2003).

#### SEE ALSO

*Air Marshals, United States*  
*Airline Security*  
*Al-Qaeda (also known as Al-Qaida)*  
*CIA (United States Central Intelligence Agency)*  
*Disinformation*  
*FAA (United States Federal Aviation Administration)*  
*FBI (United States Federal Bureau of Investigation)*  
*FEMA (United States Federal Emergency Management Agency)*  
*Iraqi Freedom, Operation (2003 War Against Iraq)*  
*Homeland Security, United States Department*  
*NTSB (National Transportation Safety Board)*  
*World Trade Center, 1993 Terrorist Attack*  
*World Trade Center, 2001 Terrorist Attack*

## Sequencing

#### ■ BRIAN HOYLE

Sequencing refers to the techniques used to determine the order of the constituent bases (i.e., adenine, thymine, guanine, and cytosine) of deoxyribonucleic acid (DNA) or protein. Protein sequencing determines the order of the constituent amino acids. Sequencing is increasingly important in forensic science and in the rapid and positive identification of potential pathogens that can be exploited by bioterrorists.

DNA is typically sequenced for several reasons: to determine the sequence of the protein encoded by the DNA, the location of sites at which restriction enzymes can cut the DNA, the location of DNA sequence elements that regulate the production of messenger RNA, or alterations in the DNA.

The sequencing of DNA is accomplished by stopping the lengthening of a DNA chain at a known base and at a known location in the DNA. Practically, this can be done in two ways. In the first method, called the Sanger-Coulson procedure, a small amount of a specific so-called

dideoxynucleoside base is incorporated in along with a mixture of the other four normal bases. This base is slightly different from the normal base and is radioactively labeled. The radioactive base becomes incorporated into the growing DNA chain instead of the normal base, growth of the DNA stops. This stoppage is done four times, each time using one of the four different dideoxynucleosides. This generates four collections of DNA molecule. Also, because replication of the DNA always begins at the same point, and because the amount of altered base added is low, for each reaction many DNA pieces of different length will be generated. When the sample is used for gel electrophoresis, the different sized pieces can be resolved as radioactive bands in the gel. Then, with the location of the bases known, the sequence of the DNA can be deduced. The second DNA sequencing technique is known as the Maxam-Gilbert technique, after its co-discoverers. In this technique, both strands of double-stranded DNA are radioactively labeled using radioactive phosphorus. Upon heating, the DNA strands separate and can be physically distinguished from each other, as one strand is heavier than the other. Both strands are then cut up using specific enzymes, and the different sized fragments of DNA are separated by gel electrophoresis. Based on the pattern of fragments the DNA sequence is determined.

The Sanger-Coulson is the more popular method. Various modifications have been developed and it has been automated for very large-scale sequencing. During the sequencing of the human genome, a sequencing method called shotgun sequencing was very successfully employed. Shotgun sequencing refers to a method that uses enzymes to cut DNA into hundreds or thousands of random bits. So many fragments are necessary since automated sequencing machines can only decipher relatively short fragments of DNA about 500 bases long. The many sequences are then pieced back together using computers to generate the entire DNA genome sequence.

Protein sequencing involves determining the arrangement of the amino acid building blocks of the protein. It is common to sequence a protein by the DNA sequence encoding the protein. This, however, is only possible if a cloned gene is available. It still is often the case that chemical protein sequencing, as described subsequently, must be performed in order to manufacture an oligonucleotide probe that can then be used to locate the target gene. The most popular direct protein chemical sequencing technique in use today is the Edman degradation procedure. This is a series of chemical reactions, that remove one amino acid at a time from a certain end of the protein (the amino terminus). Each amino acid that is released has been chemically modified in the release reaction, allowing the released product to be detected using a technique called reverse phase chromatography. The identity of the released amino acids is sequentially determined, producing the amino acid sequence of the protein.

Another protein sequencing technique is called fast atom bombardment mass spectrometry, or FAB-MS. This

is a powerful technique in which the sample is bombarded with a stream of fast atoms, such as argon. The protein becomes charged and fragmented in a sequence-specific manner. The fragments can be detected and their identity determined. The expense and relative scarcity of the necessary equipment can be a limitation to the technique.

Still another protein sequencing strategy is the digestion of the protein with specialized protein-degrading enzymes called proteases. The shorter fragments that are generated, called peptides, can then be sequenced. The problem then is to order the peptides. This is done by the use of two proteases that cut the protein at different points, generating overlapping peptides. The peptides are separated and sequenced, and the patterns of overlap and the resulting protein sequence can be deduced.

#### ■ FURTHER READING:

##### BOOKS:

Cirincione, Joseph, Jon B. Wolfsthal, Miriam Rajkuman, Jessica T. Mathews. *Deadly Arsenal: Tracking Weapons of Mass Destruction*. Washington, DC: Carnegie Endowment for International Peace, 2002.

##### PERIODICALS:

- Balding D. J. "The DNA Database Search Controversy." *Biometrics* 2002 Mar; 58(1): 241-4.
- Henderson J. P. "The Use of DNA Statistics in Criminal Trials." *Forensic Sci Int*. 2002 Aug 28; 128(3): 183-6.
- Mullis, K. B. and F. A. Faloona. "Specific Synthesis of DNA in vitro via a Polymerase catalysed Chain Reaction." *Methods in Enzymology* no. 155 (1987): 335-50.

##### SEE ALSO

*Anthrax Weaponization*  
*Biological Weapons, Genetic Identification*  
*Genetic Information: Ethics, Privacy and Security Issues*  
*Genetic Technology*  
*Genomics*  
*Infectious Disease, Threats to Security*

---

## Serbia, Intelligence and Security

---

Following the dissolution of Yugoslavia in 1989, after the fall of Soviet communism in Eastern Europe, the Balkan region fell into conflict. The former Yugoslav provinces splintered into several independent nations, but Serbia and Montenegro chose to remain a communist dominated state. The Federal Republic of Yugoslavia, as the nation was renamed, is wholly dominated by Serbia.

When civil war erupted in neighboring Bosnia-Herzegovina, Serbia provided aid to ethnic Serb forces in the region. The international community protested the move, and Yugoslav leader, Slobidan Milosevic signed a peace accord with neighboring Bosnia and Croatia. In 1999, Serbia refused to restore autonomy to Kosovo. Conflict lingered, and reports that Serbian forces were perpetrating grievous human rights crimes against Muslim Kosovars, including mass murder and deportation, prompted NATO intervention in the region. Following a bombing campaign against Serbian strongholds, peacekeeping troops entered the region.

Following the Kosovo conflict, Serbians ousted Milosevic in a general election. Vojislav Kostunica was the first non-communist leader elected in Yugoslavia in nearly 60 years. Though tension remains high in the region, and periodic violence continues to erupt, Kostunica and his government are committed to democratizing the national government and reforming the economy. The function of the national intelligence community has changed dramatically because of reforms.

The Serbian intelligence community maintains traditional distinctions between internal and foreign, civilian and military intelligence, and organizes its various agencies accordingly. However, many of these agencies' expressed duties overlap. To avoid confusion and facilitate cooperating and data sharing, the Council for Security coordinates all intelligence and security operations relating to the protection of national interests.

Though individual branches of the military maintain their own intelligence units, the Ministry of Defense oversees the largest military intelligence agencies and coordinates the intelligence and security operations of various departments and units. The *Kontraobavesajna Sluzba* (KOS), General Staff Security Directorate, provides domestic security and counterintelligence analysis for the military. The agency works closely with Military Police to insure the safety and security of Serbian military installations.

Civilian intelligence forces fall under the jurisdiction of the Ministry of the Interior. The *Sluzba Javne Bezbednosti* (SJB), Public Security Service is charged with the protection of public welfare. The SJB guards diplomatic officials and aids intelligence services with anti-terrorism operations. The future of this organization, as well as its parent, the State Security Service (SDB), is unknown. Government officials have reformed the organization several times, stripping it of its powers to conduct espionage for political reasons.

In 2000 the government created a special anti-terrorist unit, the ATJ. The group is trained in both civilian espionage and military battle techniques. The special unit was granted a wide range of operation, from intelligence to policing.

The structure of the Yugoslavian intelligence community is sure to change in the near future, as the government

continues reforms. Serbian intelligence and security agencies have cultivated a regional reputation for brutality over the past six decades, a problem that democratic reformers seek to rectify. The new government arrested Milosevic and sent him to stand trial for war crimes and crimes against humanity. The international tribunal convicted Milosevic. Since the elections of Kostunica and Prime Minister Zoran Djindjic, the nation has made strides to join the international community and participate in European economic and security organizations.

On March 12, 2003, Djindjic, one of the primary leaders of Serbia's reform movement, was assassinated by an unknown sniper.

#### SEE ALSO

*Cold War (1972–1989): The Collapse of the Soviet Union European Union*

---

## Sex-for-Secrets Scandal

---

■ DAVID TULLOCH

On December 14, 1986, a United States Marine who had been serving as an Embassy guard in Moscow and Vienna turned himself in to CIA officials. The Marine, Sergeant Clayton J. Lonetree, claimed that he had given classified information to a KGB agent with the codename "Uncle Sasha." Immediately, a government investigation was launched into the affair, as officials searched for evidence that Lonetree had not been working alone, or was just one of many Embassy guards who was successfully targeted by the Soviets.

**Violetta and 'Uncle Sasha.'** Lonetree, a Winnebago Indian from St. Paul, Minnesota, had been a model soldier. He enlisted at age eighteen in the Marine Corps, and later underwent the difficult, elite training of the Security Guard Battalion School, from which he graduated in 1984. Lonetree was then assigned to the U.S. Embassy in Moscow, and later to the Vienna Embassy. While everyday duty as an Embassy guard can be repetitive, it is a key position, and often includes access to sensitive material, such as keys to offices or safes.

It was while stationed in Moscow that Lonetree met Violetta Sanni (sometimes given as Seina), a local Russian who worked as a translator, while attending the annual Marine ball held at the Ambassador's residence in November 1985. Lonetree began to date Violetta, despite the Marine Corps prohibition against guards having close contacts with Soviet citizens, and he seems to have fallen in love with her. Sanni then introduced Lonetree to "Uncle



Christine Keeler, a call girl involved with British War Minister Lord John Profumo in a 1963 “sex for secrets” scandal, was also entangled with a Soviet spy trying to discover British nuclear secrets. ©BETTMANN/CORBIS.

Sasha,” later identified as Alexi Yelsimov. At first Lonetree enjoyed the visits of Sasha, and they talked together about Lonetree’s home, what his life had been like in the United States and on various political topics. However, Sasha was a KGB operative and he began to ask Lonetree questions.

Despite his concern, Lonetree continued to see Violetta and befriend Sasha, without notifying his superiors until the end of his Moscow tour. He was reassigned to the Vienna Embassy, where he was unexpectedly joined by Uncle Sasha. The KGB agent became Lonetree’s only contact with Violetta, giving the lonely soldier photos and packages from Moscow, and passing on Lonetree’s letters and gifts. Sasha used this new position as go-between to persuade Lonetree to provide documents and information from the embassy. Lonetree admitted to giving Sasha an old embassy phonebook and floor plans, for which he was paid \$1,800. The Marine also provided details on suspected intelligence agents working undercover in the embassy.

**Confession and conviction.** Uncle Sasha began to demand more information from Lonetree, even suggesting a trip to Moscow for KGB training and to see Violetta again. Lonetree decided he had had enough, and turned himself in to the

CIA. Nine months of intensive investigations began by the Naval Criminal Investigative Service (NCIS) and other agencies, which led to an additional five other Marine guards being detained on suspicion of espionage, lying to investigators, and improper fraternization with foreign nationals.

One of these detainees was Corporal Arnold Bracy, who was also suspected of having a romantic liaison with a Soviet woman and being an accomplice of Lonetree’s. Bracy signed a confession that stated he had helped commit a number of serious breaches of security. Bracy later claimed not to have read the document before signing it and to have signed under duress. A key claim in the confession was that Bracey and Lonetree had worked together to facilitate tours of the Moscow Embassy for KGB agents and allow them to plant listening devices. This allegation was denied by both Bracy and Lonetree, and it became evident that, working together, it would have been difficult for the two soldiers to show KGB agents through the embassy without being detected by other guards or electronic security measures. Eventually, all charges against Bracy were dropped. However, Lonetree was convicted on all of the thirteen charges he faced, becoming the first U.S. Marine to be found guilty of espionage.

**Doubts surface.** Lonetree was sentenced to 30 years in prison in November 1987 as well as a reduction in rank to private, the loss of all military pay and privileges, a \$5000 dollar fine, and a dishonorable discharge. Even so, some doubts were raised about the NIS investigation, as a number of the accusations leveled against Lonetree, Bracy, and others were later shown to be unfounded.

In 1991, Lonetree returned to court asking that his conviction be overturned. In the U.S. Court of Military Appeals, lawyers claimed that Lonetree’s confession had been inappropriately used as evidence against him, as it had been taken on the understanding that it would remain confidential. It was also suggested that Lonetree’s lawyers at his original trial had been incompetent, as they had not informed their client of the possibility of a plea agreement. Additionally, they argued that Lonetree’s cooperation should have earned him a drastically reduced sentence.

During Lonetree’s trial, it was noted that one witness had remained anonymous, which was a violation of the defendants basic right “to know the identity of the witness against him.” The witness, a CIA agent, had mostly testified in closed session. As well, military courts have procedures that differ from civil courts. At one time, it was even claimed that Lonetree had purposefully only given the KGB non-vital information, as he was planning to become a double agent.

While Lonetree’s thirty-year sentence was not overturned, the court did agree that it should be reduced. In May 1988 the term had been shortened by five years for

the cooperation he had shown investigators. Then in October 1992 another five years reduction was given. After the unsuccessful appeal, yet another shortening of five years' was granted in July 1994. In 1996, after serving just under nine years in jail, Lonetree was released early for good behavior.

The material that Lonetree passed to the KGB was not considered of great significance, and one report suggested the security implications were probably minimal. However, by coming forward, Lonetree revealed significant security lapses within the embassy staff structure that sparked changes in procedures and improved security in embassies across the world.

#### ■ FURTHER READING:

##### BOOKS:

Barker, Rodney. *Dancing with the Devil: Sex, Espionage, and the U.S. Marines—The Clayton Lonetree Story*. New York: Simon & Schuster, 1996.

Headley, Lake, and William Hoffmann. *The Court Martial of Clayton Lonetree*. New York: Henry Holt, 1989.

Kessler, Ronald. *Moscow Station: How the KGB Penetrated the American Embassy*. New York: Scribner's, 1989.

##### SEE ALSO

*Cold War (1972–1989): The Collapse of the Soviet Union Navy Criminal Investigative Service (NCIS)*  
*Reagan Administration (1981–1989), United States National Security Policy*

## Ships Designed for Intelligence Collection

#### ■ JUDSON KNIGHT

The concept of using ships as modern intelligence-gathering platforms evolved, along with larger modern ideas of intelligence operations in general, from World War II. The Cold War saw the deployment, on both the Soviet and American sides, of ships tasked with gathering communications and electronic intelligence. Some of these were disguised as fishing vessels, a practice common on the Soviet side, while the United States favored vessels operating under the guise of research craft. During the 1960s, United States ships designed for intelligence collection figured in a number of unfortunate incidents that contributed to the end of the seaborne passive electronic intelligence (ELINT) program.

**The Soviet Union.** Due to their relative lack of electronic listening posts overseas—in comparison to the Americans, who possessed signals intelligence (SIGINT) facilities throughout the world—the Soviets initially took the lead in the use of ships to gather intelligence. From the 1950s, they began using what came to be their preferred intelligence-gathering craft, a fishing trawler. The design of the trawler, which was made to store many days' catch in insulated compartments, made it ideal for extensive activities below deck.

As the Cold War continued, the Soviets expanded and improved their intelligence-collection ships, known to U.S. intelligence as AGIs, the AG being code for "miscellaneous auxiliary" and the *I* a designator of enemy craft. Later models were designed and built specifically to serve as collection platforms. Eventually they became large enough to include on-board intelligence processing facilities, greatly improving the speed with which raw data became usable intelligence for Soviet operatives.

During the Vietnam War, a pair of Soviet AGIs, one near Guam and the other in Vietnam's Gulf of Tonkin, kept a close watch on U.S. forces, and in some cases may have provided Hanoi with advance notice of U.S. airstrikes. Near the end of the Cold War, the Soviets had a fleet of about five dozen AGIs dispatched throughout the globe. A particular area of interest lay just to the east of Florida, in international waters and close to friendly ports in Cuba, from which Soviet AGIs could monitor activities at U.S. naval bases in South Carolina, Georgia, and Florida.

**The United States.** Among the few places where the United States, like the Soviet Union, lacked sufficient electronic listening posts were South America and Africa, to which the first U.S. spy ships were deployed in the early 1960s. Most such craft were cargo ships from World War II, converted by the National Security Agency (NSA) into craft for gathering SIGINT, particularly ELINT. Ships in this first phase of the U.S. maritime intelligence-gathering effort were designated T-AG, or civilian miscellaneous auxiliary craft.

Simultaneous with the T-AG phase was that of AGTR, or technical research craft. The U.S. Navy and Marines, in collaboration with NSA, operated these craft, which NSA had also converted from war-era cargo ships that had been converted. The first AGTR, *Oxford*, provided information on movement of Soviet arms into Cuba in the build-up toward the missile crisis of 1962.

**ELINT ships in history.** Of the five AGTR craft, the best was the *Liberty*, which in June 1967 was off the coast of the Sinai Peninsula. During the Six-Day War, Israeli air and naval craft, mistaking it for an enemy ship, attacked and sank it, killing 34 men and wounding 171 more. Israel later apologized and paid damages to the families of those

killed. A dozen studies by U.S. and Israeli authorities each concluded that the regrettable incident was simply a result of confusion in the midst of heavy fighting.

Two other intelligence-gathering craft also figured in well-known events. One of these was the destroyer *Maddox*, part of an ELINT-gathering mission known as DESOTO, conducted in the Gulf of Tonkin in 1964. (The *Maddox*, operating openly as a naval vessel, was not part of the AG series.) After North Vietnamese gunboats fired on it on August 4, Congress hastily passed the Tonkin Gulf Resolution, which greatly increased the scope of U.S. involvement in Vietnam.

In the meantime, the Navy and NSA, taking a page from the Soviets' book, developed the AGER (environmental research) series, using trawler-based designs for craft smaller than AGTRs. The second of three AGER craft was the *Pueblo*, captured by the North Koreans in January 1968. The *Pueblo* incident, coming as it did on the heels of the *Liberty* tragedy, brought an end to the large-scale U.S. deployment of maritime intelligence-gathering ships equipped with passive ELINT capabilities.

#### ■ FURTHER READING:

##### BOOKS:

- Holmes, W. J. *Double-Edged Secrets: U.S. Naval Intelligence Operations in the Pacific During World War II*. Annapolis, MD: Naval Institute Press, 1979.
- Packard, Wyman H. *A Century of U.S. Naval Intelligence*. Washington, D.C.: Naval Historical Center, 1996.
- Parker, James E. *Codename Mule: Fighting the Secret War in Laos for the CIA*. Annapolis, MD: Naval Institute Press, 1995.
- Polmar, Norman, and Thomas B. Allen. *Spy Book: The Encyclopedia of Espionage*. New York: Random House, 1998.
- Tourison, Sedgwick D. *Secret Army, Secret War: Washington's Tragic Spy Operation in North Vietnam*. Annapolis, MD: Naval Institute Press, 1995.

##### SEE ALSO

*Intelligence*  
*NMIC (National Maritime Intelligence Center)*  
*Pueblo Incident*  
*SIGINT (Signals intelligence)*  
*Undersea Espionage: Nuclear vs. Fast Attack Subs*  
*USS Liberty*  
*Vietnam War*

Airlines aircraft bound from Paris to Miami flight with 197 people on board. Reid attempted to destroy the flight with plastic explosives concealed in his shoes that were capable of blowing a hole in the plane's pressurized fuselage. Passengers and crew subdued Reid after the smell of burned matches alerted them to Reid's failed attempts to light his shoes.

Authorities at the Charles de Gaulle airport in Paris had failed to check Reid's shoes—not a common pre-flight security practice at the time. Subsequent to Reid's attempt, the checking of shoes and more extensive checks for explosive residues became part of pre-flight security examinations.

Charles de Gaulle (CDG) airport had an established reputation as a "soft" entry point for terrorists. In an unrelated case occurring the year after Reid's arrest, an Algerian-born CDG baggage handler who had worked at the airport for more than three years—and who had broad access to secure areas—was arrested after weapons and explosive devices (an automatic handgun, a machine gun, five bars of plastic explosives, and two detonators) were discovered in the trunk of his car.

Prosecutors subsequently asserted that "Reid's intentions were clear he wanted to murder innocent people in the name of his fanatical religious beliefs." Reid subsequently confessed and admitted guilt to eight felony charges, including attempted murder, attempted murder using a weapon of mass destruction, planting an explosive device on an aircraft, attempted destruction of an aircraft, and two counts of interfering with a flight crew.

Reid, son of an English mother and Jamaican father, was a British citizen with a history of petty crime. He converted to radical Islam while in a British jail. Reid claimed he was an enemy of the United States, and avowed his allegiance to al-Qaeda leader Osama bin Laden.

References to an al-Qaeda operative with a similar operational history and profile to Reid were found on a computer hard drive allegedly used by al-Qaeda leaders in Afghanistan.

Reid attempted to claim he was a "soldier" in the war on terrorism. At Reid's sentencing, U.S. federal judge William Young dismissed his assertions and, citing Reid's attempts to kill innocent civilians, flatly told Reid, "You are not a soldier, you are a terrorist." Reid was sentenced to life in prison without the possibility of parole.

#### ■ FURTHER READING:

##### PERIODICALS:

Ferdinand, P. "Would-Be Shoe Bomber Gets Life Term." *Washington Post*. January 31, 2003; A1.

##### SEE ALSO

*Airline Security*

---

## "Shoe Bomber"

---

On December 22, 2001, al-Qaeda sympathizer Richard Reid attempted the mid-flight destruction of an American

*Terrorist Organization List, United States  
Terrorist Organizations, Freezing of Assets  
Terrorist Threat Integration Center*

## Shoe Transmitter

A popular weekly situation comedy called “Get Smart” ran on the American Broadcasting Corporation television network in the United States for five seasons in the 1960s. In the show—a spoof of spies and espionage organizations—the lead character, Maxwell Smart, often communicated with his colleagues via a “shoe phone.” The television series and the espionage equipment were conceived as a nonsensical spoof of the spy movies that were in vogue at that time. Nonetheless, the shoe phone was grounded in reality.

During the Cold War, with tensions arising between the United States and the former Soviet Union in the 1950s and 1960s, both nations conducted espionage campaigns to collect information from the other country that was deemed vital to national security. As part of these efforts, the Soviet spy agency known as the KGB (Komitet Gosudarstvennoi Bezopasnosti, which translates as the Committee for State Security) devised a microphone and transmitter that could be concealed in a shoe.

The shoe transmitter could detect conversation in the immediate vicinity and broadcast the conversation to a receiver located in a nearby secret monitoring station. Essentially, the shoe transmitter was a tiny radio station, broadcasting on a frequency that would be detected only by the special receiver.

The shoe transmitter was intended to eavesdrop on conversations of someone who could supply important and privileged information. A pair of dress shoes designed to be worn for business purposes—one of which contained the microphone and transmitter in a hollow heel—was planted in the home, hotel room, or office of the subject. This was done by someone affiliated with the KGB who had ready access to the subject such as a maid, valet, or co-worker. When the shoes were planted, a pin located in a hollowed-out heel was pulled out. This activated the radio beacon and the microphone, allowing conversation to be recorded until the batteries that powered the equipment ran out of power.

With the coming of more sophisticated bugging technologies in the 1970s, the use of the shoe transmitter was phased out. However, at the time the device was a sophisticated piece of equipment and demonstrated that miniaturization of electronic hardware was possible.

Unlike its comedic counterpart, the device could not be used to make telephone calls.



A shoe with an imbedded heel transmitter produced by the KGB during the Cold War to monitor secret conversations. ©AFP/CORBIS.

A copy of the shoe transmitter is now on display at the International Spy Museum. The museum opened in July 2002 in Washington, D.C.

### ■ FURTHER READING:

#### ELECTRONIC:

International Spy Museum. “Collections Overview.” <<http://www.spymuseum.org/media/collections.html>> (20 December 2002).

#### SEE ALSO

*Audio Amplifiers  
Bugs (Microphones) and Bug Detectors  
Parabolic Microphones*

## Short-Wave Transmitters

Short-wave radio transmission and reception occurs in the range somewhere between 2 and 30 MHz (megahertz, or million cycles per second). Because these signals are capable of propagating over a greater distance than either AM or FM radio, shortwave is the preferred medium for radio broadcasting to remote locations. World powers in the twentieth century and beyond made use of short-wave radio transmissions to bridge political and physical barriers in sending propaganda messages to distant populations.

Despite their name, shortwaves are relatively long in wavelength compared to most of the electromagnetic spectrum. They measure anywhere from 33 to 262 feet (10–80 m), gargantuan in comparison to ultra high-energy waves such as x rays and gamma rays, of which it would take many millions to cover even the length of a millimeter. On the electromagnetic spectrum, the higher the energy level, the higher the frequency, and the shorter the wavelength.

Shortwaves shorter than AM (amplitude modulation) radio waves, to which the U.S. Federal Communications Commission has assigned the frequency range of 535 kHz to 1.7 MHz. Short-wave transmissions occur somewhere between 2 to 5.9 MHz at the low end, and 26.1 to 30 MHz at the high end. Above these are microwave regions assigned to television stations, as well as FM, which occupies the range from 88 to 108 MHz. Like AM signals, those of short-wave radio transmissions propagate over a great distance because they bounce off of a heavily charged layer in the earth's ionosphere.

The length of signal propagation prompted the establishment of international short-wave communications in the late 1930s. During the Cold War, the world's major powers used shortwave to transmit propaganda messages. Examples of these efforts included the short-wave stations operated by Voice of America, Radio Moscow, Radio Beijing, and the British Broadcasting Corporation.

Long before the 2003 invasion of Iraq, the United States, through its Central Intelligence Agency, supported Iraqi short-wave stations operated by resistance movements. In June 1996, President William J. Clinton provided \$6 million to the Iraqi National Accord, which set up several stations, including Twin Rivers Radio, Radio Tikrit, and al Mustaqbal. The latter, whose name means "The Future," broadcast from Kuwait and from U.S. military EC-130 psychological operations planes, on the frequency of 1575.3 kHz (1.5753 MHz), which in the United States would be a high-frequency AM station.

#### ■ FURTHER READING:

##### BOOKS:

Helms, Harry L. *Shortwave Listening Guidebook: The Complete Guide to Hearing the World*. Solana Beach, CA: High Text Publications, 1993.

McCormick, Anita Louise. *Shortwave Radio Listening for Beginners*. Blue Ridge Summit, PA: TAB Books, 1993.

Yoder, Andrew R., and Hank Bennett. *The Complete Short-wave Listener's Handbook*. New York: McGraw-Hill, 1997.

##### ELECTRONIC:

Clandestine Radio.com. <<http://www.clandestineradio.com>> (April 2, 2003).

##### SEE ALSO

*CIA, Foreign Broadcast Information Service*

*Electromagnetic Spectrum*

*National Telecommunications Information Administration, and Security for the Radio Frequency Spectrum, United States*

*Propaganda, Uses and Psychology*

## Shredding.

SEE *Document Destruction*.

## SIGINT (Signals Intelligence)

■ JUDSON KNIGHT

Signals intelligence, or SIGINT, is one of the four major forms of intelligence, along with human, imagery, and measurement and signatures intelligence (HUMINT, IMINT, and MASINT respectively). As its name suggests, it is intelligence derived from the interception of signals, including communications signals, electronic emissions, and telemetry. The two major subsets of SIGINT are COMINT, or communications intelligence, gained through the interception of foreign communications (excluding open radio and television broadcasts); and ELINT or electronics intelligence, derived from the interception of non-communication electromagnetic signals, most notably radar.

Communications intercepts may be in the form of voice transmissions via telephone or radio, Morse code, teletype, or facsimile machine. In the modern intelligence environment, most such communications are encrypted, and typically require sophisticated computer technology for decryption. A major component of efforts by the intelligence services of the English-speaking world is Echelon, a worldwide system of satellites, interception stations, and supercomputers jointly operated by the United States, United Kingdom, Canada, Australia, and New Zealand. The U.S. National Security Agency (NSA) takes the lead in this and many other COMINT efforts.

Early U.S. efforts in SIGINT would today be placed under the heading of COMINT. Although the U.S. Army conducted cryptography and cryptanalysis prior to 1930, concerted efforts began in that year with the establishment of the U.S. Army Signal Intelligence Service (SIS), which consolidated all such operations. Notable activities of SIS included the breaking of the Japanese Foreign Ministry PURPLE cipher prior to World War II. SIS, renamed several times during the war, was replaced in 1945 by the Army Security Agency (ASA). In 1977, the Army Intelligence and Security Command (INSCOM) replaced



ASA. The Navy had its own COMINT activities, later taken over by NSA.

**ELINT.** All intercepts of non-communication signals sent over electromagnetic waves, excluding those from atomic detonations (which are the province of MASINT operations), fall under the heading of ELINT. In World War II, the Allies conducted ELINT operations involving Axis air defense radar systems, to neutralize these in a bombing raid, either through a direct hit or by electronic countermeasures. Since that time, the United States has targeted or monitored the radar operations of numerous enemies, including the Soviet Union and China during the Cold War, North Vietnam during the war in Southeast Asia, and Libya and Iran during latter-day conflicts in the Middle East.

The radar component of ELINT is not to be confused with RADINT, or radar intelligence from nonimaging radar. Unlike ELINT, RADINT does not involve the interception or radar signals; instead, intelligence regarding flight path and other specifics is derived from the deflection of enemy radar signals. RADINT is a subcategory of MASINT.

**FISINT and TELINT.** Actual varieties of ELINT include FISINT, or foreign instrumentation signals intelligence, and its subcategory, TELINT, or telemetry intelligence. The signals sent by foreign entities when testing and deploying aerospace, surface, and sub-surface systems—examples include tracking and aiming signals, as well as video data links—are the material of FISINT operations.

Telemetry is the process of making measurements from a remote location and transmitting those measurements to receiving equipment. It has extensive civilian and military applications. As an example of the former, an electric company may use radio signals from remote power lines to relay operational information to the center of the power grid. Among the military applications of telemetry is the use of signals to relay information on the performance of a guided missile system.

#### ■ FURTHER READING:

##### BOOKS:

- Aldrich, Richard J. *The Hidden Hand: Britain, America, and Cold War Secret Intelligence*. Woodstock, NY: Overlook Press, 2002.
- Alvarez, David J. *Allied and Axis Signals Intelligence in World War II*. Portland, OR: F. Cass, 1999.
- Andrew, Christopher M. *Codebreaking and Signals Intelligence*. Totowa, NJ: F. Cass, 1986.
- Bennett, Richard M. *Espionage: An Encyclopedia of Spies and Secrets*. London: Virgin Books, 2002.
- Gilbert, James L., and John Patrick Finnegan. *U.S. Army Signals Intelligence in World War II: A Documentary*

*History*. Washington, D.C.: U.S. Government Printing Office, 1993.

Richelson, Jeffrey T. *The U.S. Intelligence Community*, fourth edition. Boulder, CO: Westview Press, 1999.

Sexton, Donal J. *Signals Intelligence in World War II: A Research Guide*. Westport, CT: Greenwood Press, 1996.

West, Nigel. *The SIGINT Secrets: The Signals Intelligence War, 1900 to Today: Including the Persecution of Gordon Welchman*. New York: W. Morrow, 1988.

#### SEE ALSO

- COMINT (Communications Intelligence)*  
*Echelon*  
*Electronic Countermeasures*  
*HUMINT (Human Intelligence)*  
*IMINT (Imagery Intelligence)*  
*Intelligence*  
*Measurement and Signatures Intelligence (MASINT)*  
*NSA (United States National Security Agency)*  
*Special Relationship: Technology Sharing Between the Intelligence Agencies of the United States and United Kingdom*  
*Telemetry*

## Silencers

■ CARYN E. NEUMANN

A silencer is an effort to suppress sound by means of an attachment to a firearm. Generally, a six- to twenty-inch steel, titanium, or aluminum alloy barrel addition designed to work with a particular weapon, silencers have also been constructed from other materials such as plastic soft drink bottles. Nicknamed “whispering death,” these devices give a shooter the ability to strike a target with less risk of being noticed. Contrary to popular image, silencers do not completely muffle the sound of a gun, but instead lessen muzzle flash, reduce muzzle noise, and decrease recoil by delaying the escape of gases from the barrel of the firearm. Generally illegal for individuals to own in most parts of the world, silencers have enjoyed enormous popularity with espionage and security forces.

The idea of a silencer is an old one, with gunsmiths experimenting with various designs to silence weapons since the nineteenth century. The first man to successfully develop and market a silencer was Hiram P. Maxim, the son of the similarly named inventor of the machine gun. In 1908, Maxim developed a silencer that delayed the release of gases, but he did not market the weapon until making a few improvements. The Maxim Model 1909, released in the year of its name, became the first efficient silencer to be marketed, but the Maxim Model 1910 became the most widely distributed silencer in the United States by capitalizing on an off-center design that allowed it to be used with



A Hungarian soldier fires an AK-47 style assault rifle equipped with a silencer. ©LEIF SKOOGFORS/CORBIS.

a weapon's original sights. Although the military value of silencers quickly became apparent to many observers, Maxim only had the goal of eliminating noise pollution. Many of the first buyers of silencers employed them for target shooting in basements and backyards so the sound of firing would not disturb others. Silencers also found a market in pest control. Many silencers are still sold for use in eliminating rats, not so much to surprise the rodents, but to avoid the public relations problems associated with shots fired in heavily occupied areas.

Despite global marketing by Maxim, no nation's military force made widespread use of silencers until World War II. The Maxim Model 1912 was the first mass-marketed silencer designed specifically for military purposes. Created for use with the popular Springfield rifle, the report of the weapon was reduced, but the sonic boom of the bullet could not be diminished. The passage of the bullet sounded like someone tearing a sheet until the projectile passed a solid object, like a tree, which resulted in the emission of a large crack. The 1912 model was not sold to any government in great numbers, perhaps because of the notorious conservativeness of military planners in this era, but it did find a few buyers. The U.S. Army purchased a few of the weapons to be used by sharpshooters for the quiet, long-range killing of sentries so that surprise attacks could be mounted. The silencers were

apparently used in Mexico in the campaign against Pancho Villa, but, because the Army failed to halt Villa, the effectiveness of the silencers is somewhat in doubt. In World War I, Maxim manufactured silencers in calibers ranging from .22 through those large enough for machine guns. An experimental model silenced a four-inch artillery piece. Snipers continued to be the major users of silencers, though, and these men used only rifles. The Germans experimented with a silencer-equipped Luger pistol, but the gun suffered mechanical failure as well as too high a noise rate. In the years after the war, public interest in silencers waned, and Maxim halted production in 1925.

In the years between the World Wars, silencers failed to find a substantial market among any of the world's military forces. The U.S. military conducted a number of trials with silencers, but ultimately decided that the weapons were unfit for combat use. Despite the silenced discharge, the substantial noise created by the movement of gun parts enabled observers to easily locate the bulky weapons. While unsuitable for normal military usage, silencers appealed to intelligence agencies and these organizations continued to experiment with the weapons. The United States Office of Strategic Services (OSS), newly formed to help fight World War II, modified the Thompson submachine gun with a silencer built by the Chrysler Corporation. The gun proved too noisy to be suitable for a

silencer as well as very susceptible to jamming under field conditions. The OSS preferred to equip its agents with a silenced version of the M3 submachine gun in addition to a .30 caliber M1 carbine. The Central Intelligence Agency, successor to the OSS, used a silenced High Standard HD military pistol. Francis Gary Powers, pilot of the U-2 reconnaissance plane shot down over the Soviet Union in 1960, carried the silenced HD when he was captured. Around the world, the Welrod became a weapon of first choice. One of the few silencers designed specifically for silent and secret operations, the British-built gun was produced in .32 ACP, 9mm, and .45 ACP calibers.

When firing a standard weapon, some sort of ear protection must be utilized or temporary loss of hearing will result. Plugs and earmuffs reduce noise level, but also make it much more difficult to hear movement. Silencers make it much easier to locate and fire upon multiple targets, and this factor explains the expanding popularity of the weapons. After World War II, silencers were increasingly used in combat conditions. A silencer confuses the person being fired upon, improves the shooter's accuracy by suppressing disconcerting flash, noise, and recoil and, lastly, gives the shooter a feeling of confidence that he will not be discovered. The M3A1, an improved M3, became popular in various global hotspots like Greece, Africa, Palestine, and South America because the cheap and easy-to-build weapon usually could be relied upon to work. In the 1950s Allied forces, as well as British commandos, used the British-made Sten MKIIS in the Korean War. In the Vietnam era, the U.S. created a military version of a Ruger 10–22 semi-automatic Carbine that saw heavy use. In more recent years, military snipers have used a great variety of rifle makes in combat, though the AK-47 remains especially popular.

The development of a supremely effective silencer has been complicated by many factors. The noise made by the discharge of a firearm has three components: 1) the sounds made by the movement of the parts of the gun; 2) the crack of a bullet passing through the atmosphere at a rate above the speed of sound; and 3) the release of high pressure gases breaking out of the barrel. Silencers only address the last concern, although the use of a heavy subsonic bullet rather than a high velocity bullet greatly adds to sound suppression. High velocity bullets make a noise of their own when traveling through the air outside of the silencer, and the substitution of a slower bullet will slow the passage of the projectile through the air, thereby reducing ballistic noise. Silencers that fire regular supersonic ammunition are only a little quieter than those without suppressors. Subsonic ammunition has less power than regular ammunition, making it effective only at shorter ranges of up to 600 feet (200 meters). Silencers can be attached to most firearms, but they work best as components of purpose built or modified guns.

Silencers are now made for almost every firearm, from fully automatic submachine guns to big bore bolt-action rifles, and the popularity of these weapons is likely to grow. Silencers make it easier to identify the enemy, easier to shoot the enemy, and harder to be detected by

the enemy. Particularly suited for guerrilla warfare as well as secret operations and law enforcement, sound suppressors have become standard issue equipment for intelligence agents and security forces.

#### ■ FURTHER READING:

##### BOOKS:

Truby, J. David. *Silencers, Snipers and Assassins: An Overview of Whispering Death*. Boulder, CO: Paladin Press, 1972.

White, Mark. *On the Control of Silencers, Interpol: The International Criminal Police Organization*. Washington, D.C.: Government Printing Office, 2002.

##### SEE ALSO

*Assassination Weapons, Mechanical*  
*CIA (United States Central Intelligence Agency)*  
*Espionage*  
*Intelligence Agent*  
*OSS (United States Office of Strategic Services)*  
*U-2 Incident*

---

## Skunk Works

---

“Skunk Works” is the nickname for the headquarters of advanced development programs for Lockheed Martin Aeronautics Company at Palmdale, California, some 80 miles (128 km) north of Los Angeles in the Antelope Valley. Established in 1943 by what was then known as the Lockheed Aircraft Corporation, the Skunk Works has been the birthplace of numerous extraordinary aircraft, including the U-2 and SR-71 reconnaissance planes and the F-117A stealth fighter.

During World War II, Lockheed established the facility, under the direction of Clarence L. (Kelly) Johnson, to build the ultra-secret P-80 Shooting Star, the first jet-propelled fighter in the U.S. air fleet. The Skunk Works got its name from a nearby chemical plant, the noxious odors of which wafted toward the Lockheed facility on windy days. Technicians there referred to the plant as the “skunk works,” a term taken from the comic strip *L’il Abner* by Al Capp, and eventually the nickname became attached to the facility itself.

Over the decades that followed, the Skunk Works produced the U-2 in the 1950s, the A-12 Oxcart and SR-71 Blackbird in the 1960s, and the F-117A Nighthawk in the 1980s. It also adapted the C-130, used for troop transport by airborne forces, for special missions. The Skunk Works even built a ship, the U.S. Navy research vessel *Sea Shadow*.

In addition, engineers at the Skunk Works developed the CL-282 and CL-400, two craft that were never went into use. The first of these, introduced in 1958, was to be a high-altitude reconnaissance craft, but plans for it were



NASA selected the Lockheed-Martin Skunk Works to build and test the technology demonstrator VentureStar, as shown in this computer-generated concept. Skunk Works emerged from the cloak of secrecy that has shrouded it since the Cold War. AP/WIDE WORLD PHOTOS.

scrapped in favor of the U-2. The CL-400 was to be a successor to the U-2, based on Johnson's design for a hydrogen-powered supersonic craft. However, the results satisfied neither Lockheed nor the Air Force, and the project was abandoned in October 1957.

#### ■ FURTHER READING:

##### BOOKS:

- Bennis, Warren G., and Patricia Ward Biederman. *Organizing Genius: The Secrets of Creative Collaboration*. Reading, MA: Addison-Wesley, 1997.
- Jenkins, Dennis R. *Lockheed Secret Projects: Inside the Skunk Works*. St. Paul, MN: MBI Publishing, 2001.
- Miller, Jay. *Lockheed Martin's Skunk Works*. North Branch, MN: Specialty Press, 1995.
- Pace, Steve. *Lockheed Skunk Works*. Osceola, WI: Motorbooks International, 1992.
- Rich, Ben R., and Leo Janos. *Skunk Works: A Personal Memoir of My Years at Lockheed*. Boston: Little, Brown, 1994.

##### ELECTRONIC:

Lockheed Martin Aeronautics Company. <<http://www.Imaeronautics.com/palmdale/>> (April 2, 2003).

##### SEE ALSO

*F-117A Stealth Fighter*  
*Photography, High-Altitude*  
*SR-71 Blackbird*  
*U-2 Spy Plane*  
*Vietnam War*

## Slovakia, Intelligence and Security

The security and intelligence agencies of Slovakia work in the shadow cast by their communist-era predecessors. In

a situation common among many nations of the former Soviet bloc, Western observers have noted a distressing degree of continuity between the old police-state security and intelligence apparatus, and that of the new democratic state. At the same time, Slovakia has worked to fulfill the requirements of integration into the new, post-communist Europe.

In 1993, Slovakia separated from the Czech Republic, with which it had comprised the nation of Czechoslovakia. Citizens of that nation had, during the years of communist rule, come to fear the State Security Service, or StBU. By 1993, the StBU had been disbanded, but four years later, Radio Free Europe reported that much of the infrastructure of the StBU lingered on under the guise of the new Slovenska Informacna Sluzba (Slovak Information Service, or SIS). According to the American information service, the Slovak government regularly conducted surveillance operations on its citizenry through the SIS.

A decade later, Slovakia was under consideration for membership in both the European Union (EU) and the North Atlantic Treaty Organization (NATO), both of which require democratization as a prerequisite for admission. At the same time Slovakia had progressed toward greater democracy, its security and intelligence services had improved their ability to protect sensitive secrets. Among the requirements NATO imposed was the establishment of the National Security Office (NBU), which officially began operating in November 2001. The purpose of NBU is, in part, to protect classified information, which is shared between member nations.

In December 2002, members of the European Union approved Slovakia for membership in the EU beginning in 2004.

#### ■ FURTHER READING:

##### BOOKS:

Williams, Kieran, and Dennis Deletant. *Security Intelligence Services in New Democracies: The Czech Republic, Slovakia, and Romania*. New York: Palgrave, 2001.

##### PERIODICALS:

Gill, Peter. Review of *Security Intelligence Services in New Democracies: The Czech Republic, Slovakia, and Romania*. *Slavic Review* 61, no. 2 (2002): 375–76.

##### ELECTRONIC:

Naegele, Jolyon. Slovakia: Intelligence Service Reverts to Communist-Era Practices. Radio Free Europe/Radio Liberty. <<http://www.rferl.org/nca/features/1997/05/F.RU.97052913316.html>> (March 1, 2003).

Slovakia: Intelligence. Federation of American Scientists. <<http://www.fas.org/irp/world/slovakia/index.html>> (March 1, 2003).

##### SEE ALSO

*Czech Republic, Intelligence and Security*  
*Hungary, Intelligence and Security*  
*Poland, Intelligence and Security*

## Slovenia, Intelligence and Security

The principal intelligence agency in Slovenia is the *Slovenska Obvesčevalno-Varnostna Agencija* (SOVA; Slovenian Intelligence and Security Agency). Domestic security priorities set by the national assembly guide SOVA, which is responsible for collecting information both at home and abroad on groups or individuals who might threaten the state and its constitutional system.

Other components of the Slovenian intelligence and security apparatus include the national defense ministry, under whose aegis are the 1st Special Brigade of the Slovenian Army, also known as the Ministry of Defense Reconnaissance and Intervention Service (MORIS), as well as the Ministry of Defense Intelligence and Security Service (VOMO). Additionally, the Ministry of the Interior, Ministry of Foreign Affairs, National Police Force, and Customs Service all have security and/or intelligence roles.

Slovenia's security depends to a large extent on the integration of policies and resources involving the United Nations, the Organization for Security and Cooperation in Europe, the European Union (EU), and NATO—especially with regard to establishing long-term stability in the Balkans.

In December 2002, members of the European Union approved Slovenia for membership in the EU beginning in 2004.

#### ■ FURTHER READING:

##### ELECTRONIC:

Slovene Intelligence and Security Agency. <<http://www.sigov.si/vrs/ang/ang-text/ministries/slovene-intelligence-and-security-agency.html>> (March 1, 2003).

Slovenia: Intelligence. Federation of American Scientists. <<http://www.fas.org/irp/world/slovenia/index.html>> (March 1, 2003).

##### SEE ALSO

*Bosnia, Intelligence and Security*  
*Croatia, Intelligence and Security*  
*Serbia, Intelligence and Security*

## Smallpox

Smallpox is an infection caused by the variola virus, a member of the poxvirus family. The disease is highly

infectious. Passage from person to person via contaminated aerosolized droplets (from sneezing, for example) occurs easily, and so the spread of smallpox through a population can occur quickly. Like most viruses and other microorganisms, the variola virus can be transported from one location to another without difficulty, thus making smallpox a potentially attractive choice for biological warfare and a serious threat as a weapon of bioterrorists.

Smallpox is a highly contagious disease. The virus can spread by direct contact with those who are infected, in contaminated air droplets, and even by touching objects such as books and blankets that have been previously used by someone who has smallpox.

When infected with the virus, there is a 12–14 day symptom-free period, during which the virus is multiplying in the body. There is then a sudden onset of symptoms. The symptoms include fever and chills, muscle aches, and a flat, reddish-purple rash on the chest, abdomen, and back. These symptoms last about three days, after which the rash fades and the fever drops. A day or two later, the fever returns, along with a bumpy rash starting on the feet, hands, and face. This rash progresses from the feet along the legs, from the hands along the arms, and from the face down the neck, ultimately reaching and including the chest, abdomen, and back. The individual bumps, or papules, fill with clear fluid, and, over the course of 10–12 days, become pus-filled. The pox eventually scabs over, and when the scab falls off it leaves behind a pock-mark or pit, which remains as a permanent scar on the skin of the victim.

Smallpox can be lethal, usually due to bacterial infection of the open skin lesions, pneumonia, or bone infections. A severe and quickly fatal form of smallpox is known as “sledgehammer smallpox.” This form of smallpox is characterized by bleeding from the skin lesions, as well as from the mouth, nose, and other areas of the body.

Smallpox has been present for thousands of years. For example, studies of the mummy of Pharaoh Ramses V, who died in 1157 B.C., revealed symptoms of smallpox infection.

Large smallpox epidemics have occurred throughout recorded history. Attempts to protect against smallpox infection began centuries ago, even though the microbiological nature of the disease was then unknown. In the tenth century, accounts from China, India, and the Americas describe how individuals who had even a mild case of smallpox could not be infected again. Fluid or pus from the skin lesions was scratched into the skin of those who had never had the illness, in an attempt to produce a mild reaction and its accompanying protective effect. Unfortunately, these efforts sometimes resulted in full-fledged smallpox, and helped spread the infection. Such crude vaccinations against smallpox were outlawed in Colonial America.

In 1798, Edward Jenner published his observation that milkmaids who contracted cowpox infection caused

by vaccinia virus (a relative of variola) were immune to smallpox. He used infected material from the cowpox lesions to prepare an injection that helped protect the humans. Although Jenner’s development of immunization was harshly criticized at first, the work paved the way for the development of vaccines.

Until the development of a smallpox vaccine, no treatment for smallpox was known, nor could anything shorten the course of the disease. Until its eradication, smallpox was diagnosed most clearly from the patients’ symptoms. Electron microscopic studies could identify the variola virus in fluid isolated from disease papules, from infected urine, or from the blood prior to the appearance of the papular rash.

In the 1960s, the World Health organization (WHO) began a campaign to treat people infected with smallpox and vaccinate those who might be exposed to the infection. The WHO program was extremely successful, and the virus was declared eradicated worldwide in May of 1980. Stored stocks of the virus were maintained in two laboratories. One is housed at the Centers for Disease Control and Prevention in Atlanta, Georgia. The other smallpox stock is maintained in Russia.

These stocks were slated to be destroyed in the late 1990s however, U.S. President William J. Clinton halted plans for destruction of the American stocks. Concern that another poxvirus could mutate (undergo genetic changes) and cause human infection, along with the possible use of smallpox as a bioterrorist weapon or as a weapon of state-sanctioned war, has made preservation of the smallpox stock for vaccine development purposes important. As of early 2003, the stocks remain undisturbed.

#### ■ FURTHER READING:

##### BOOKS:

Hopkins, D. R. *The Greatest Killer: Smallpox in History*. Chicago: University of Chicago Press, 2002.

Preston, R. *The Demon in the Freezer*. New York: Random House, 2002.

##### PERIODICALS:

Henderson, D. A., T. V. Inglesby, J. G. Bartlett, et al. “Smallpox as a Biological Weapon: Medical and Public Health Management.” *Journal of the American Medical Association* no. 281 (1999): 2127–137.

##### ELECTRONIC:

Centers for Diseases Control and Prevention. “Smallpox.” Public Health Emergency Preparedness and Response. November 26, 2002. <<http://www.bt.cdc.gov/agent/smallpox/index.asp>>(27 November 2002).

##### SEE ALSO

*Biocontainment Laboratories*

---

## Smallpox Vaccine

---

■ BRIAN HOYLE

Smallpox, or *variola major*, is a highly contagious disease that is caused by the *variola virus*. The name smallpox comes from the Latin word for spotted. A visual hallmark of smallpox is the raised bumps that appear on the victim's face and body. Smallpox is fatal in approximately 25% of cases.

There is no cure for smallpox, and treatment is supportive. Prevention of the disease by the administration of smallpox vaccine is the most effective strategy to eliminate the spread of smallpox. Vaccination, conducted on a worldwide scale, was successful in effectively eliminating smallpox as a naturally occurring disease.

The eradication of smallpox saw the end of routine vaccination programs. As of 2003, no American under the age of 30 routinely receives the vaccine. Even in older Americans, immunity has likely faded. After the bioterrorist anthrax attacks on U.S. citizens in late 2001, concern has heightened that smallpox will be used as a terrorist weapon on a population that is once again susceptible to infection. Beginning in January, 2003, health care workers at strategic hospitals and research centers across the United States received the smallpox vaccine in order to provide a population of immune responders in case of a smallpox outbreak or mass exposure due to bioterrorism. Mass vaccination programs are again under study by researchers, and smallpox vaccines are scheduled to be available to all Americans on a voluntary basis by mid-2004.

The only smallpox vaccine that is in use today—a preparation called Dryvax—is made from *vaccinia*, a poxvirus that is very similar to the smallpox virus. The reaction of the immune system to *vaccinia* confers protection to the smallpox virus. The *vaccinia* virus that is administered is alive and causes a mild infection, which is inconsequential in most people. However, in a small minority of people, the use of the live virus does carry a risk that the virus will spread from the site of injection, and that side effects will result.

The side effects are typically minor (e.g., sore arm at the injection site, a fever, and generalized body aches). However, rare severe side effects are possible, which can even be life threatening. These include encephalitis (a swelling of the brain and spinal cord), gangrene, extreme eczema, and blindness. People whose immune systems are not functioning properly are especially at risk, as are

those people who have had skin ailments such as eczema or atopic dermatitis. The fatality rate due to the vaccine is estimated to be one in eight million.

Despite the risk, smallpox vaccine is worthwhile if exposure to smallpox is possible. A single injection of *vaccinia* vaccine preparation provides up to five years of immunity to smallpox. A subsequent injection extends this protection. Studies have demonstrated that up to 95% of vaccinated people are protected from smallpox infection. Protection results after just a few days. If exposure to smallpox is anticipated—such as in a military campaign—vaccination a short time before can be a wise precaution.

Smallpox vaccine is injected using a two-pronged needle dipped into the vaccine solution, which then pricks the skin of an upper arm several times in a few seconds. The injection typically becomes sore, blisters and forms a scab. When the scab falls off, a distinctive scar is left.

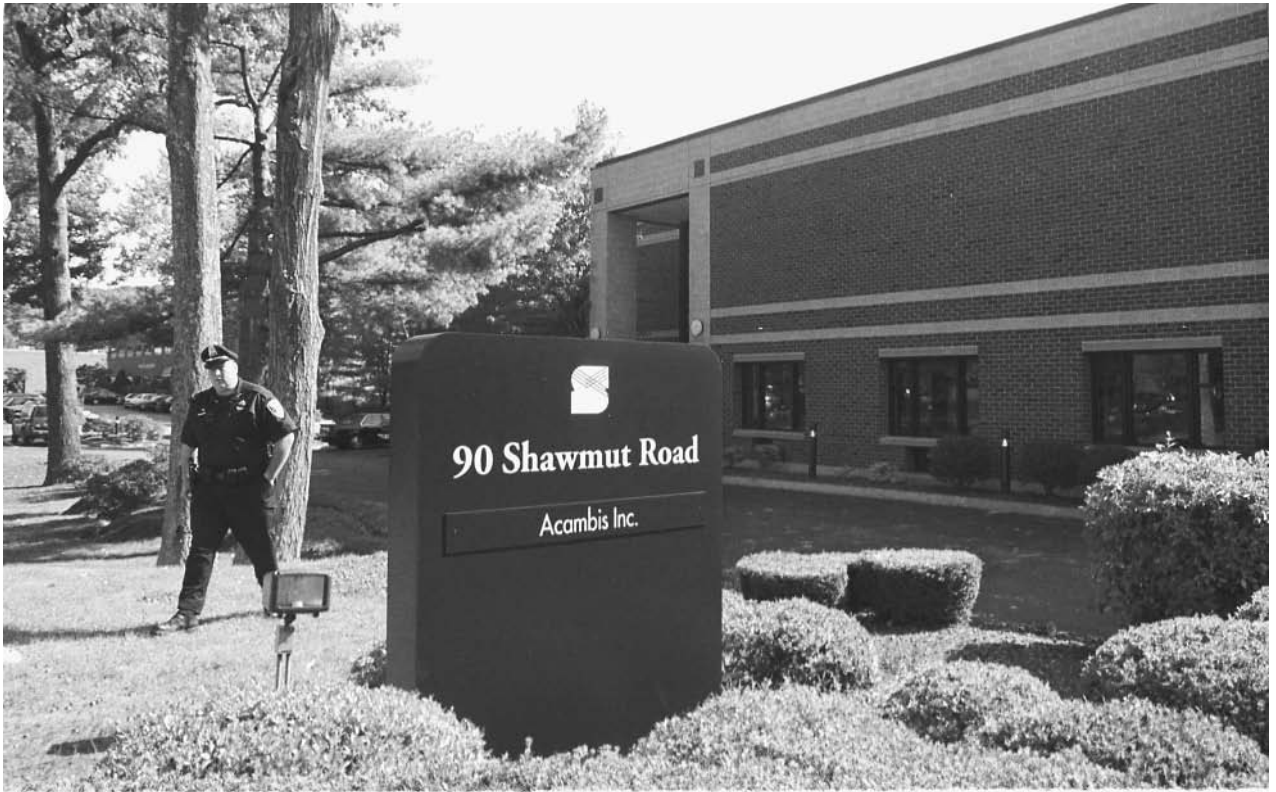
Currently, the stockpile of smallpox vaccine in the U.S. is about 15 million doses. The vaccine may be capable of being diluted 10 times without losing its protective potency. This would extend the coverage to 150 million people. As of December 2002, 155 million additional doses of smallpox vaccine are being delivered. The new vaccine is made from cow tissues that were grown in laboratory culture. This technique produces a more uniform vaccine preparation than the old method, where tissue was scraped from the lesions of infected cows.

**Other smallpox vaccines.** The development of improved smallpox vaccines, and the refinement of existing vaccine preparations, has begun only recently. Research on improved vaccines largely ended when the demand for vaccinations ended in the 1970s.

A form of smallpox vaccine called Modified *vaccinia* Ankara (MVA) was developed 40 years ago. The *vaccinia* virus used in this preparation cannot replicate in human cells, but still generates an immune response. While the vaccine appears to produce fewer side effects than the standard *vaccinia* vaccine, large scale tests have not yet been done.

Another *vaccinia* strain that has been used to develop a smallpox vaccine is called LC16m8. In contrast to MVA, LC16m8 does replicate inside human cells. However, the virus lacks some of the usual surface proteins that may be important in the immune response.

Genetic engineering is also playing a role in smallpox vaccine development. For example, a *vaccinia* strain has been engineered that does not form certain proteins unless the antibiotic tetracycline is present. The idea here is that the vaccine and the antibiotic would be taken simultaneously. In the event of an adverse vaccine reaction, use of the antibiotic would be stopped, which would stop the immune reactivity of the *vaccinia* virus. This approach is still in the laboratory stage.



A Canton, Massachusetts, police officer, left, is seen outside the offices of Acambis Inc., a licensed producer of smallpox vaccine, in October 2001. The fear of bioterrorism attacks has spurred federal officials to ask the British-owned company to speed up production of the vaccine. AP/WIDE WORLD PHOTOS.

#### ■ FURTHER READING:

##### BOOKS:

Institute of Medicine. *Assessment of Future Scientific Needs for Live Variola Virus*. Washington, DC: National Academy Press, 1999.

##### PERIODICALS:

Henderson, D.A. "Smallpox: clinical and epidemiologic features." *Emerging Infectious Diseases* no. 5 (1999): 537–39.

Rosenthal, S.R., M. Merchinsky, C. Kleppinger, et al. "Developing New Smallpox Vaccines." *Emerging Infectious Diseases* no. 7 (2001): 920–26.

##### ELECTRONIC:

Centers for Disease Control and Prevention. "Smallpox Factsheet: Vaccine Overview." Public Health Emergency Preparedness and Response. December 9, 2002. <<http://www.bt.cdc.gov/agent/smallpox/vaccination/facts.asp>>(31 December 2002).

##### SEE ALSO

*Biological Warfare*  
*Infectious disease, threats to security*  
*NNSA (United States National Nuclear Security Administration)*  
*Weapons of Mass Destruction, Detection*

## SOE (Special Operations Executive)

■ CARYN E. NEUMANN

A World War II-era British secret service division, the Special Operations Executive (SOE), formed on July 19, 1940, to coordinate subversion and sabotage in enemy-occupied countries. SOE agents distributed propaganda, blew up bridges, directed air strikes, destroyed factories, and taught resistance tactics. Most of SOE's success came in France, Yugoslavia, Greece, and Italy, although it also conducted major operations in Albania, Abyssinia, Belgium, Burma, China, Denmark, Hungary, Malaya, Norway, Poland, Romania, Siam (present-day Thailand), Turkey, and the Dutch East Indies. SOE disbanded on January 15, 1946, with many of its agents moving to MI6.

With the fall of France in 1940, SOE received authorization to begin operations to divert German, Italian, and Japanese attention away from the main fighting fronts towards the rear areas. The division, with headquarters scattered throughout London, developed three branches: SO1 for propaganda, SO2 for active operations, and SO3 for planning. Resistance movements had already formed



in occupied countries, and it fell to SOE to finance, supply, and direct these operations. It did not operate effectively in the main enemy homelands of Germany and Japan because the locals were too unfriendly and the police too strong.

In order to achieve its goals, SOE relied upon 470 agents, 117 of whom died in action. The agents generally parachuted behind the lines to teach unarmed combat, bomb building, and espionage strategies to resistance fighters, but a number were pulled from the criminal ranks to supply expertly forged documents. SOE's greatest success may have been the 1942 bombing of a Norwegian plant that supplied heavy water (deuterium oxide) to Germany for use in developing an atomic bomb. Another notable achievement came when SOE agents guided a Royal Air Force attack on Gestapo headquarters in Denmark that permitted one prisoner escaping from the rubble to pick up a file of the names of Danish collaborators to be used as evidence at treason trials after the war. SOE so succeeded in harassing the Axis powers that they pulled troops from the front lines and sent them to guard railways, storage depots, and factories, while the British in contrast simply relied upon old men to protect these facilities.

An accurate measure of SOE's impact is difficult. The requirements of clandestine work meant that SOE agents rarely left written records, and those few official papers that do exist have been classified secret by the British government. The little that is known about the division marks it as a success.

■ FURTHER READING:

BOOKS:

Foot, M.R.D. *SOE: An Outline History of the Special Operations Executive 1940–46*. London: British Broadcasting Corporation, 1984.

SEE ALSO

- Covert operations*
- Espionage*
- French Underground During World War II, Communication and Codes*
- Gestapo*
- MI6 (British Secret Intelligence Service)*
- Nuclear Weapons*
- Propaganda, Uses and Psychology*
- Sabotage*

Soldier and Biological  
Chemical Command (SBCCOM),  
United States Army

The United States Army Soldier and Biological Chemical Command (SBCCOM) is a support organization focused

on the development, response to, and safe handling of chemical weapons. Formed in 1998 from the merger of two earlier groups, SBCCOM is heavily involved in preparedness training for both military and civilians to prevent or, if necessary, respond to terrorist attacks.

In December 1998, the United States Army combined its Chemical and Biological Defense Command and its Soldier Systems Command to form SBCCOM. The new command, which brought together expertise in soldier, chemical, and biological areas, was responsible for research, development, and implementation of chemical, biological, and soldier missions. It would also oversee the chemical weapons stockpile of the United States Army from its headquarters in the Edgewood Area of the Aberdeen Proving Ground in Maryland.

**Mission.** The mission of SBCCOM is to develop, integrate, acquire, and sustain soldier and NBC [nuclear, biological, and chemical] defense technology, systems, and services to ensure the decisive edge and maximum protection for the United States. Provide for the safe storage, treaty compliance, and destruction of classified material.

To this end, the command is involved in three principal areas: research, development, and acquisition of chemical and biological weapons and defense systems; emergency preparedness and response in the event of attack; and the safe, secure storage, remediation, and demilitarization of chemical and biological weapons.

**Realizing mission objectives.** Research takes place in two principal centers. At the Edgewood Chemical Biological Center, project managers undertake concept exploration, demonstration, validation, and emergency manufacturing development for production of chemical defense systems, aerosol systems, flame weapons, and obscuring smoke. At the Soldier Systems Center in Natick, Massachusetts, SBCCOM analysts address problems of total life-cycle management for the soldier through centralized development, procurement, and integration. These issues involve matters such as shelters, airdrops, field service, and organizational equipment.

SBCCOM oversees the safe and secure storage of chemical weapons at eight depots scattered across the United States: Edgewood, Maryland; Blue Grass, Kentucky; Newport, Indiana; Anniston, Alabama; Pine Bluff, Arkansas; Pueblo, Colorado; Tooele, Utah; and Umatilla, Oregon. At these sites, SBCCOM also regulates U.S. compliance with international treaties on chemical weapons. Additionally, a post at Rocky Mountain Arsenal in Colorado is charged with safely destroying old chemical weapons.

In the area of emergency preparedness and response, SBCCOM directs the Army Technical Escort Unit, which is globally deployable and has a history that goes back to the Korean War. (Other aspects of SBCCOM activities date to the period between the world wars, which saw early

efforts to control the spread and use of the chemical weapons that had been displayed with such gruesome effect on the Western Front in World War I.) SBCCOM also leads the Domestic Preparedness Program, which in 1998 made the news with education efforts in 120 cities nationwide.

#### ■ FURTHER READING:

##### PERIODICALS:

Dezelan, Louis A. "Preparing for Terrorism." *Law & Order* 46, no. 10 (October 1998): 107–110.

Thompson, Neal. "Preparing for Disaster." *The Sun*. (Baltimore, MD) (March 13, 1998): 3B.

##### ELECTRONIC:

United States Army Soldier and Biological Chemical Command (SBCCOM). <<http://www.sbccom.army.mil/>> (January 27, 2003).

##### SEE ALSO

*Chemical Safety: Emergency Responses*

## Solid-Phase Microextraction Techniques

Solid-phase microextraction (SPME) is a chemical technique designed to detect chemical compounds. In its forensic application, it is used to find chemical warfare agents, high explosives, or illegal drugs. Among the world's leading research institutes in forensic SPME work is Lawrence Livermore National Laboratory's Forensic Science Center (FSC) in San Francisco. Established in 1991, the FSC, which had 15 staff members in 2002, implements a variety of research tools in forensics. Among these is SPME, which makes use of optical fibers to collect chemical samples.

Extremely small, these fibers are about 100 micrometers thick—the width of a human hair. Stored in syringes, they are coated with chemicals made to respond to specific substances such as particular explosives or drugs. With a minimum of disruption and effort, these "chemical dipsticks" can collect thousands of compounds.

One of the few drawbacks of the fibers used in SPME is the fact that they are extremely fragile, and for this reason, the FSC developed durable aluminum storage tubes. They have also provided the Federal Bureau of Investigation with portable SPME field kits, as well as a transport tube small enough to fit in a shirt pocket. The FSC is licensing both versions to private industry for sale to the federal government.

SPME has been used at the FSC to monitor the safety of nuclear warheads as part of the Stockpile Stewardship Program. After collecting samples of volatile and semivolatile molecules formed from the breakdown of organic polymers and high explosives, scientists look for signs that corroded parts may need to be replaced.

#### ■ FURTHER READING:

##### PERIODICALS:

Bodrain, Rosemarie R. "Analysis of Exempt Paint Solvents by Gas Chromatography Using Solid-Phase Microextraction." *JCT, Journal of Coatings Technology* 72, no. 900 (January 2000): 69–74.

Comello, Vic. "Researchers Are Giving SPME a Second Look." *Research & Development* 41, no. 2 (February 1999): 44–45.

Marsili, Ray. "New Techniques Revolutionize Analyses of Liquid Samples." *Research & Development* 42, no. 2 (February 2000): 22–24.

##### ELECTRONIC:

Counterterrorism and Incident Response. Lawrence Livermore National Laboratory. <<http://www.llnl.gov/nai/rdiv/rdiv.html>> (April 2, 2003).

Solid-Phase Microextraction (SPME). Science & Technology, Lawrence Livermore National Laboratory. <[http://www.cms.llnl.gov/s-t/solid\\_phase.html](http://www.cms.llnl.gov/s-t/solid_phase.html)> (April 2, 2003).

##### SEE ALSO

*Chemistry: Applications in Espionage, Intelligence, and Security Issues*  
*Forensic Science*  
*Gas Chromatograph-Mass Spectrometer*  
*Lawrence Livermore National Laboratory (LLNL)*

## Soman

#### ■ BRIAN HOYLE

Soman (or "GD") is a synthetic (human-made) compound that affects the functioning of nerves. As such, Soman is one of a group of chemicals that are known as nerve agents.

Soman was developed in Germany in 1944. Its original purpose was as an insecticide. The chemical, which does not occur naturally in the environment, is similar to the group of insect poisons (pesticides) called organophosphates, both in activity and in how they are applied (i.e., airborne release). However, Soman (and nerve agents in general) are much more potent and deadly than the insect nerve poisons.

Several properties of Soman are responsible for its potency. It is normally a clear, colorless, and tasteless liquid, and so is not easily detected. While it typically has a slight odor reminiscent of rotting fruit, this smell can be disguised upon mixing with water or food. Even wetting

the skin with soman-contaminated water can be lethal, as the poison is absorbed through the skin. In addition, Soman can vaporize when heated, and retains its toxicity when inhaled. The vapor can even cling to clothing and affect others as is it released from the clothing.

The effects of Soman begin almost immediately upon exposure. Within minutes to hours the nerves that control the functioning of muscles are inhibited from turning off the stimuli that trigger muscle activity. At the molecular level, this occurs via the inactivation of an enzyme that breaks apart another chemical that acts as a bridge between adjacent nerve cells, and so allows a nerve impulse to flow. Because the bridging chemical remains intact, nerve impulses cannot be controlled or turned off. As a result of the constant activity, muscles such as the lungs tire and can cease to function. Some of the symptoms associated with Soman exposure include watery and painful eyes, coughing, rapid breathing, diarrhea, confusion, headache, slow or fast heart rate, and, in severe cases, unconsciousness, convulsions, and respiratory failure.

These effects occur for only a short time after Soman vapor is released into the atmosphere, since it is a very volatile compound. When incorporated into water or food, however, Soman can remain active and deadly for a longer time.

The damage due to Soman is cumulative. Because the chemical can persist in the body, repeated exposure increases the concentration of Soman in the body. People in low-lying areas and valleys can be especially susceptible, as Soman is more dense than air and so “settles out” near the bottom of depressions.

Soman was one of the nerve agents that may have been used against the people of Iran by the government of Iraq under Saddam Hussein during the Iran-Iraq war in the 1980s. Soman once also once produced as a chemical weapon by the United States. Production by the United States ceased decades ago.

#### ■ FURTHER READING:

##### BOOKS:

Government of the United States. *21st Century Complete Guide to Chemical Weapons and Chemical Terrorism—U.S. Demilitarization Program, Stockpile Destruction Emergency Plans, Nerve Gas and Blister Agent Civilian Treatment and First Aid, Home Sheltering Plans*. Washington, DC: Progressive Management, 2002.

##### ELECTRONIC:

Agency for Toxic Substances and Disease Registry. “Nerve Agents (GA, GB, GD, VX).” Division of Toxicology, Centers for Disease Control and Prevention. March 13, 2003. <<http://www.atsdr.cdc.gov/factsd4.html>>(April 10, 2003).

Agency for Toxic Substances and Disease Registry. “Facts about Soman.” Division of Toxicology, Centers for Disease Control and Prevention. March 12, 2003. <<http://www.bt.cdc.gov/agent/soman/basics/facts.asp>>(April 10, 2003).

#### SEE ALSO

*Chemical Warfare*  
*Mustard Gas*  
*Sarin Gas*

## SONAR

■ K. LEE LERNER

SONAR, an acronym for Sound Navigation and Ranging, is a technique based on echolocation used for the detection of objects underwater.

**Historical development of SONAR.** Ancient drawings depict the use of long tubes as non-mechanical underwater listening devices to detect and transmit sound in water. In the late nineteenth century, scientists began to explore the physical properties associated with sound transmission in water. In 1882, a Swiss physicist, Daviel Colladen, attempted to calculate the speed of sound in the known depths of Lake Geneva. Based upon the physics of sound transmission articulated by English physicist Lord Rayleigh (1842–1914), and the piezoelectric effect discovered by French scientist Pierre Curie (1509–1906), in 1915, French physicist Paul Langevin (1872–1946) invented the first system designed to utilize sound waves and acoustical echoes in an underwater detection device.

In the wake of the *Titanic* disaster, Langevin and his colleague Constantin Chilowsky, a Russian engineer then living in Switzerland, developed what they termed a “hydrophone” as a mechanism for ships to more readily detect icebergs (the vast majority of any iceberg remains below the ocean surface). Similar systems were put to immediate use as an aid to underwater navigation by submarines.

Improved electronics and technology allowed the production of greatly improved listening and recording devices. Because passive SONAR is essentially nothing more than an elaborate recording and sound amplification device, these systems suffered because they were dependent upon the strength of the sound signal coming from the target. The signals or waves received could be typed (i.e. related to specific targets) for identifying characteristics. Although skilled and experienced operators could provide reasonably accurate estimates of range, bearing, and relative motion of targets, these estimates were far less precise and accurate than results obtained from active systems unless the targets were very close—or were very noisy.

The threat of submarine warfare during World War I made urgent the development of SONAR and other means of echo detection. The development of the acoustic transducer that converted electrical energy to sound waves

enabled the rapid advances in SONAR design and technology during the last years of the war. Although active SONAR was developed too late to be widely used during World War I the push for its development produced enormous technological dividends. Early into World War II, the British Anti-Submarine Detection and Investigation Committee (its acronym, ASDIC, became a name commonly applied to British SONAR systems) made efforts to outfit every ship in the British fleet with advanced detection devices. The use of ASDIC proved pivotal in the British effort to repel damaging attacks by German submarines.

**SONAR and RADAR.** Although they rely on two fundamentally different types of wave transmission, SONAR and Radio Detection And Ranging (RADAR) and both are remote sensing systems. While active SONAR transmits acoustic (i.e., sound) waves, RADAR sends out and measures the return of electromagnetic waves.

In both systems these waves return echoes from certain features or targets that allow the determination of important properties or attributes of the target (e.g., shape, size, speed, distance to target, etc.). Because electromagnetic waves are strongly attenuated (diminished) in water, RADAR signals are mostly used for ground or atmospheric observations. Because SONAR signals easily penetrate water, they are ideal for navigation and measurement under water. Within the ocean, the speed of sound varies with changes in temperature and pressure, and these conditions can also be determined by alterations in SONAR signals.

SONAR usually operates at frequencies in the 10,000–50,000 Hz range. Higher higher frequencies provide more accurate location data, but propagation losses (i.e. loss of signal strength over distance) also increase with frequency.

#### ■ FURTHER READING:

##### BOOKS:

Van Trees, Harry L. *Radar-Sonar Signal Processing and Gaussian Signals in Noise*. Indianapolis, IN: John Wiley & Sons, 2001.

Waite, A. D. *Sonar for Practising Engineers*. Indianapolis, IN: John Wiley & Sons, 2001.

##### ELECTRONIC:

Canadian Center for Remote Sensing, "History of Remote Sensing." 2001. <<http://www.ccrs.nrcan.gc.ca/ccrs/org/history/morleye.htm>> (February 1, 2003).

##### SEE ALSO

*P-3 Orion Anti-Submarine Maritime Reconnaissance Aircraft*

*Remote Sensing*

*SOSUS (Sound Surveillance System)*

*Undersea Espionage: Nuclear vs. Fast Attack Subs*

## SOSUS (Sound Surveillance System)

■ K. LEE LERNER

Utilizing the unique properties of sound transmission in water, during the 1950s, the United States Navy developed the Sound Surveillance System (SOSUS). Code named "Jezebel" the SOSUS system provided critical monitoring of Soviet submarine and ship movements, especially through the critical ocean gaps between Greenland, Iceland, and the United Kingdom (the GI-UK gap). SOSUS systems were so sensitive that trained observers could determine ship type—and in some cases, identify specific ships.

SOSUS used arrays of hydrophones (underwater microphones) strategically placed along the ocean bottom. The hydrophones were connected by cables to onshore monitoring stations.

In addition to localized sound readings (i.e., sounds detected within the expected range of the hydrophones), SOSUS also picked up sounds channeled through specific conditions of state (i.e., pressure, temperature) or salinity that create channels through which sound waves propagate over long distances with minimal resistance and minimal loss of strength. This sound fixing and ranging channel (SOFAR channel) was discovered independently by American and Soviet scientists in 1943 during World War II.

SOFAR channels are capable of transmitting the low frequency, long wavelength sound waves produced by an explosion. Sound waves can be trapped effectively in SOFAR channels and propagate with little loss of energy over distances in excess of 15,500 miles (25,000 km).

Naval communication systems utilize low frequency, long wavelength signals to enhance communications with submerged submarines. Prior to the widespread use of Global Positioning System (GPS) equipment, the SOFAR channel was also used for navigation and the location of marine craft. Evidence gathered by marine biologists indicates that certain species of whales utilize the SOFAR channel to communicate mating calls over long distances.

In general, the speed of sound depends upon the medium through which the sound waves propagate and the properties of the medium (e.g., state, temperature, pressure, salinity, etc.) Accordingly, the speed of sound differs in air, fresh water, and oceanic saltwater.

Within the ocean, the speed of sound varies with changes in temperature and pressure. When the near-surface layer is well mixed by currents and surface action, the resulting isothermal layer provides uniform propagation of sound. When a temperature gradient exists (e.g., a temperature decrease with increasing depth), the resulting thermocline shows a characteristic decrease in the

speed of sound with decreasing temperature. At some depth (approximately 420 fathoms or 750 meters), the variations in temperature become so slight that the water becomes isothermal. As depth increases, so does the pressure. Because pressure is directly proportional to sound wave transmission speeds, as the pressure increases with depth so does the speed of sound.

Specific combinations of temperature, pressure, and salinity may act to create “shadow zones” that are resistant to the propagation of sound waves or that act as reflectors of sound waves. Soviet submarine captains attempted to use these zone or layer to conceal their ships from detection by surface SONAR arrays. The layers could also to “bend” signals detected by the SOSUS array in order to attempt to conceal ship movements. In practice, staying within such layers proved impossible to maintain for extended periods, and intermittent SOSUS plots could be used to track ship movements or provide a probable position to explore with the use of sonar buoys dropped by airplane.

Surface sonar buoys were also used to fill gaps in the SOSUS listening network.

#### ■ FURTHER READING:

##### BOOKS:

Munk W., Worcester P., and C. Wunsch. *Ocean Acoustic Tomography*. Cambridge: Cambridge University Press, 1995.

##### SEE ALSO

*P-3 Orion Anti-Submarine Maritime Reconnaissance Aircraft*  
*Undersea Espionage: Nuclear vs. Fast Attack Subs*

---

## South Africa, Intelligence and Security

---

After decades of segregation under the system of apartheid, South Africa in 1994 became a multiracial democracy. In place of the old regime, which included the dreaded Bureau of State Security—BOSS, a agency portrayed memorably by British author Graham Greene in *The Human Factor* (1978)—the new South Africa had its own intelligence and security organizations. Included among these are the National Defense Force Intelligence Division, the National Intelligence Agency (NIA), the South African Police Service (SAPS), the South African Secret Service (SASS), and the National Intelligence Coordinating Committee (NICOC), which oversees these agencies.

The South African National Defense Force (SANDF) consists of four military organizations—army, navy, air force, and medical service—as well as support services. It was formed from the integration of the old South African Defense Force with the armies of the three former racial homelands (Transkei, Bophuthatswana, and Venda), as well as those of political parties, including the African National Congress (ANC), Pan Africanist Congress (PAC), Umkhonto weSiswe, and the Azanian People’s Liberation Army. Similarly, NIA was formed from a combination of the old National Intelligence Service with the intelligence services of ANC, PAC, and the three former homeland intelligence services, and the ANC and PAC. Likewise SAPS is an amalgam of the old South African Police and 10 former homeland agencies.

The SANDF Intelligence Division collects and evaluates military intelligence, and supplies this as needed to national leadership. NIA is charged with collecting domestic intelligence concerning persons or groups who may potentially threaten the security of the republic or its people. Among the special units of SAPS are the Crime Combatting and Investigation Division; the National Investigative Service, whose roles include counterintelligence work with NIA; the Visible Policing Division, a crime-prevention organization; and the Special Guard Unit, which performs a bodyguard function similar to that of the U.S. Secret Service. SASS conducts foreign intelligence and counterintelligence operations.

NICOC, which reports to the president and cabinet, brings together the Coordinator for Intelligence, the Director-General of NIA, the chief of the National Defense Force Intelligence Division, the head of the National Investigation Service of SAPS, and the Director-General of SASS. It thus serves as a “joint chiefs of staff” for the South African intelligence community.

#### ■ FURTHER READING:

##### BOOKS:

McCarthy, Shaun. *Intelligence Services for a Democratic South Africa: Ensuring Parliamentary Control*. London: Research for the Study of Conflict and Terrorism, 1996.

Winter, Gordon. *Inside BOSS: South Africa’s Secret Police*. London: Allen Lane, 1981.

##### PERIODICALS:

Mallet, Victor. “Pretoria Faces German Bugging Protest.” *Financial Times* (November 22, 1999): 10.

“Thabo’s Watching: Spying in South Africa.” *The Economist* 362, no. 8266 (March 30, 2002): 41.

##### ELECTRONIC:

South African Department of Defence. <<http://www.mil.za/>> (March 1, 2003).

South African Intelligence Agencies. Federation of American Scientists. <<http://www.fas.org/irp/world/rsa/index.html>> (March 1, 2003).

## South Korea, Intelligence and Security

South Korea, or the Republic of Korea (ROK), has an intelligence and security apparatus that is, in many respects, modeled on that of the United States. The ranking system in the defense forces is similar to that of the U.S. Army, Navy, Air Force, and Marines, and the Presidential Security Service (PSS) performs a role similar to that of the U.S. Secret Service. The National Intelligence Service (NIS) was even known as the Korean Central Intelligence Agency (KCIA) from 1961 to 1981. On the other hand, the police system in the ROK is quite unlike that of the United States.

In addition to an army, navy, air force, and marine corps, the ROK military includes the Homeland Reserve Force. Overseeing the entire military structure are two executive bodies, the National Security Council and the Ministry of Defense. Military intelligence across all branches is the work of the Defense Security Command, formed in 1977 from a merger of the Army Security Command, the Navy Security Unit, and the Air Force Office of Special Investigations.

Though some of these units had names identical to agencies in the U.S. Army, the model for the DSC and its predecessor organizations was the system in Taiwan, or the Republic of China (ROC), where the Guomindang Party had political officers monitoring the military services. The ROK and ROC have similar political histories. Both represent democracy in divided nations whose other portion—North Korea and the People's Republic of China respectively—is communist. Yet both systems were, until near the end of the twentieth century, notorious in the West for the limitations they placed on individual liberties. Both have since experienced liberalization efforts that, in the ROC, led to the end of the one-party Guomindang rule, and in the ROK, reduced the power of the chief intelligence agency.

Created in 1961, KCIA had a mission combining that of the United States CIA and the Federal Bureau of Investigation, though its power in domestic affairs—including virtually unlimited authority to arrest and imprison—was far greater than that of its American counterparts. After KCIA chief Kim Chae-gyu assassinated the dictatorial President Park Chung Hee in 1979, KCIA experienced a purge and loss of power. It emerged in 1981 as the Agency for National Security Planning (ANSP), which still exerted enormous influence. ANSP's role in the 1987 torture and death of student dissident Pak Chong-ch'ol helped spark a move for greater democratization. This ultimately resulted in the 1999 dissolution of ANSP in favor of the National Intelligence Service, which is more clearly subordinated to the national assembly.

In the ROK, there is no local police system; rather, all police are under the authority of the National Police Agency. The latter exerts its authority from the capital in Seoul, where it controls five special-task police agencies, including marine police, and thirteen provincial police headquarters.

### ■ FURTHER READING:

#### BOOKS:

Kim, Jin-hyun, and Chung-in Moon. *Post-Cold War, Democratization, and National Intelligence: A Comparative Perspective*. Seoul: Yonsei University Press, 1996.

#### ELECTRONIC:

South Korea Intelligence and Security Agencies. Federation of American Scientists. <<http://www.fas.org/irp/world/rok/index.html>> (March 1, 2003).

#### SEE ALSO

*Japan, Intelligence and Security*  
*North Korean Nuclear Weapons Programs*  
*Korean War*  
*North Korea, Intelligence and Security*  
*Taiwan, Intelligence and Security*

## Soviet Union (USSR), Intelligence and Security

### ■ ALEXANDR IOFFE

On December 20, 1917, less than two months after the October Social Revolution in Russia, the All-Russian Special Commission for Combating Counter-revolution and Sabotage (VChK) was created in the new Soviet Russia. The agency was created by decree of the Council of the People's Commissar (SNK), the government at that time, "for combating counter-revolution and sabotage." The main aim of the commission was the suppression of any opposition to the new regime in any form, and in this case "suppression" very often meant physical extermination of persons who did not approve the regime. In September 1918, the SNK promulgated the decree that came to be known as the "Red Terror." Officially, the red terror was provoked by the increasing activity of the opposition that threatened the emerging Soviet government. The decree served as a basis for purging opposition, however, and punishing perceived enemies of the Soviet power by isolation in concentration or work camps. The VChK began an organized campaign to capture perceived enemies of the state, imprison them, or often, execute them without benefit of a trial.



The *Liman*, center, an intelligence-gathering vessel of Russia's Black Sea Fleet, sails through the Bosphorus Strait in 1999 on a mission to gain information about conflicts among the Balkan states. AP/WIDE WORLD PHOTOS.

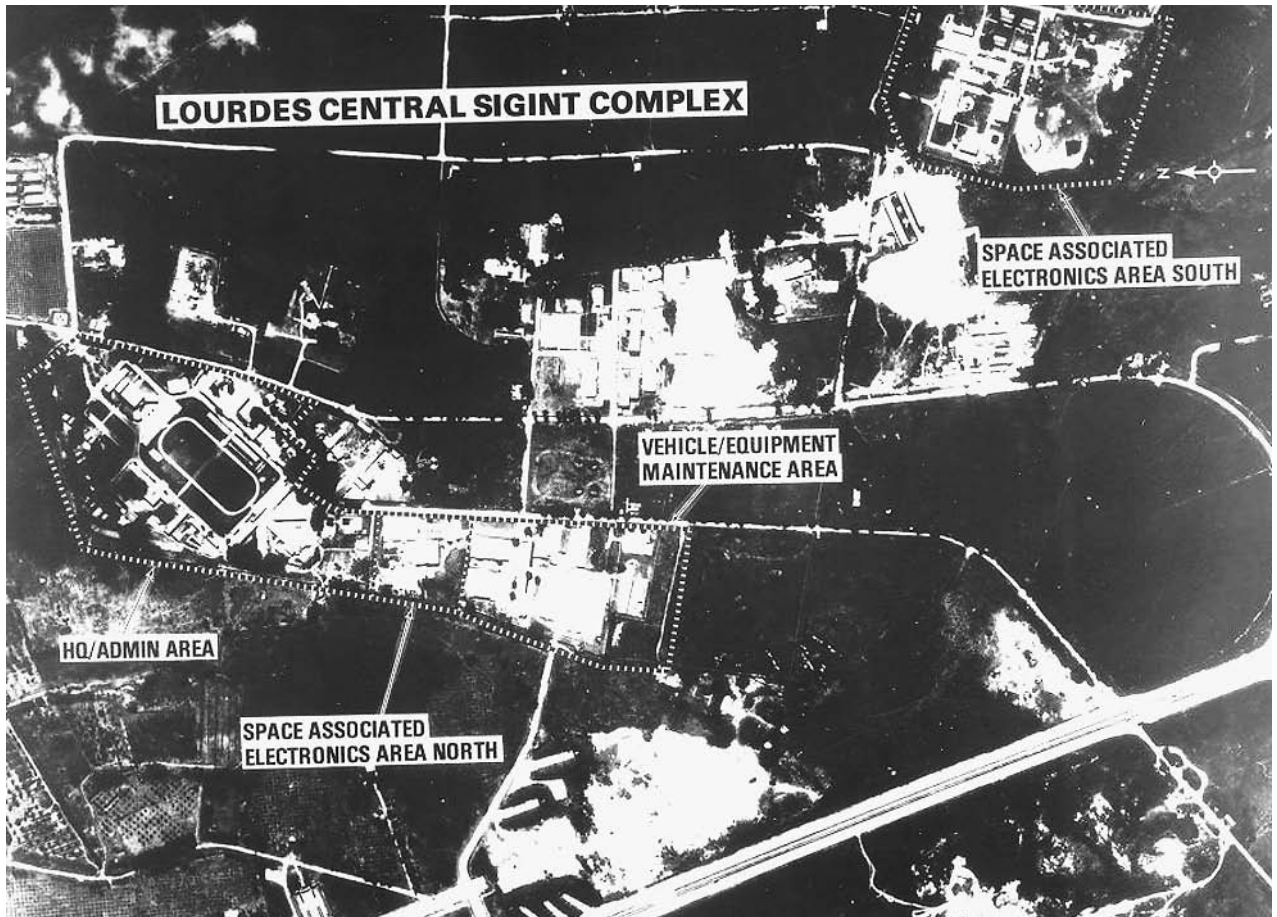
In February 1922, the VChK was formally abolished, but it was practically reorganized as the State Politic Administration of NKVD, and in November 1923, it was reorganized again as the Joint State Politic Administration (OGPU) of the SNK. Felix Dzerzhinskii, a former professional revolutionary born in Poland, headed these structures until his death in 1926. Compared to the VChK, the OGPU's activities enlarged, as it began to engage not only in problems of internal security of the regime, but also in problems of intelligence and active work abroad. The Foreign Department (INO) was created within the OGPU in December 1920, for the purpose of conducting intelligence and subversive activities in foreign countries. In this work, the OGPU cooperated actively with the Comintern, the Communist International, whose leaders were in Moscow, and which was under total control of the Communist Party of the Soviet Union.

The People's Commissariat of Home Affairs (NKVD) was also organized in 1917 in Soviet Russia to handle the security concerns of the new regime. The country's police force (officially named "militia") reported to the NKVD. Functions of the NKVD and successors of the VChK often

became entangled, and during the period from the 1920s until the beginning of World War II, these two organizations operated both jointly and separately. In 1934, the new "All-Union" People's Commissariat of Home Affairs (known again as the NKVD) was created. The new NKVD included the Main Agency of State Security (GUGB), which was the successor of the OGPU. The new NKVD also included the central agency of Militia (police), the border and internal guards, and the fire guards.

A notorious arm of the NKVD was the main agency responsible for labor camps and deportation, the Gulag. Activities of the infamous Gulag were described in detail in the works of the Nobel Prize-winning Soviet dissident and work camp prisoner Alexander Solzhenitsyn. The Gulag interred millions of political prisoners in camps throughout the Soviet Union, and became infamous for its cruel methods of suppression.

From September 1936, until December 1938, the head of the NKVD was Nikolai Ezhov, who became infamous for his efficient cruelty. During this period of purges ordered by the Soviet leader Joseph Stalin and known as the Great Terror, over 1.5 million Soviet citizens were arrested for



The Kremlin learned of U.S. battle plans for the 1991 Persian Gulf War through its electronic spy network based in Cuba and known as Lourdes, seen in this photo taken by a U.S. spy plane. AP/WIDE WORLD PHOTOS.

crimes against the state. Almost half of those arrested were executed by gunfire. Although acting under direct orders from Stalin, this period is often referred to as "Ezhovshina," meaning Ezhov's time. Eventually, Ezhov himself was arrested and executed, as Stalin grew suspicious of Ezhov's knowledge and tactics. Ezhov was replaced by Lavrenti P. Beria, who served as the head of the NKVD, along with other Soviet security agencies until 1953, when Beria was arrested and shot for attempting to gain power after the death of Stalin. The Great Terror continued under Beria, with the numbers interned in the Gulag work camps estimated between 4 and 20 million by the end of 1939.

Also before World War II, Soviet intelligence gave serious attention to suppressing political enemies of the regime. Probably the best-known example of such activity is the assassination of Leon Trotsky, the main political enemy of Stalin and one of the leaders of the Russian Revolution. Trotsky was deported from the USSR in 1929; he roamed from country to country seeking political refuge, finally settling in Mexico. Soviet secret services tried to murder him several times according to Stalin's order. At

first, the Russians used Mexican communists in the attempts to murder Trotsky. In one such attempt, the famous Mexican painter David Siqueiros participated. A group of Mexicans with machine guns riddled Trotsky's bedroom with bullets one night, then escaped, assuming that Trotsky was dead. Trotsky and his wife, however, were alerted, and hid safely under the bed. After this assassination attempt, Trotsky supporters guarded his home. Finally, the Russian NKVD agent Ramon Merkader befriended Trotsky's secretary, and through her unknowing confidence, gained access to the Trotsky home carrying an ice-axe, and carried out the assassination of on August 20, 1940.

The Komitet Gosudarstvennoy Bezopasnosti (KGB), or Committee for State Security, was the primary organization during the Soviet period for intelligence and counterintelligence matters, although it often played a role in maintaining domestic security alongside the NKVD. In the years of the new Soviet Republic before World War II, some people in Western countries supported communism and cooperated with the KGB for ideological reasons. One famous example of such cooperation is the case



of the “Cambridge five.” Soviet intelligence drew upon the sympathies and cooperation of five students at Cambridge University (Kim Philby, Donald McLean, Guy Burgess, John Carincross, and Anthony Blunt) to recruit them as spies in the 1930s. After World War II, several members of the spy ring attained key positions in the British intelligence service, where they gained access to many of Britain’s most guarded secrets. Led by Philby, components of the spy ring fed Western intelligence secrets to the Soviets for over a decade after the war. After they were exposed, MacLean and Burgess defected to the Soviet Union in 1949; Philby escaped detection and functioned in his role as double agent until 1963, when he also defected and became a colonel in the KGB. Both Blunt and Carincross escaped detection and remained in Britain until the 1990s, when they were exposed by the British government.

During World War II, the activity of all Soviet intelligence and secret services became much more active; old agent ties were restored and new ones were created. Counter-intelligence and strategic data connected with the war activity were obtained. After the end of the war the “atomic espionage” began. And along with this, the concentration camps continued to exist in the country, and new repressive tasks appeared. Stalin, for example, ordered the exile of entire nations (e.g., the Crimean Tartars, the Chechens), and this order was executed strictly.

Activities of the Soviet secret services remained acute after World War II. In 1954, the famous State Security Committee (KGB) was again created after reorganization, which conducted intelligence and repressive activities along with other information gathering. The head of the KGB enjoyed an important position in the totalitarian regime hierarchy, and one, Yuri Andropov, even became the head of the Soviet state. KGB leaders played an important role in the attempt to overthrow the government of the first (and last) president of the USSR, Mikhail Gorbachev, when they isolated Gorbachev in the Crimea for three days during his vacation in August, 1991.

The KGB was essentially abolished after the failure of the anti-Gorbachev putsch and the collapse of the USSR in 1991. The following agencies were created from within the KGB: the Federal Security Service (FSB); the Federal Agency of Government Intercommunication, which is responsible for communications between top state officials; the Guard Service, which guards top state officials; and the Outer Intelligence Service, which collects and processes all data coming from abroad.

Immediately after the Red (Soviet) Army was created in the early twentieth century, its own intelligence was organized, and by 1917, the Department of Agitation and Intelligence of the General Staff was operational. With the increasing power of the Army, its intelligence strengthened, and before World War II, the Intelligence agency of the Red Army was formally organized in 1934, and later reorganized again into the Main Intelligence Agency (GRU). The Soviet Army Intelligence existed until the collapse of the USSR, and today exists in the Russian Army. In the end of the Soviet epoch, this Agency was the most powerful

intelligence structure, and executed different tasks of both strategic and operative intelligence with large networks of agents abroad and representatives in practically in every Soviet embassy. The GRU had its own dedicated troops and unofficially competed with the KGB for power and prestige in the Soviet government.

#### ■ FURTHER READING :

##### BOOKS:

Janseen, Marc, and Nikita Petrov. *Stalin’s Loyal Executioner: People’s Commissar Nikolai Ezhov 1895–1940*. Palo Alto, CA: Hoover Institution Press, 2002.

Knight, Amy. *Beria: Stalin’s First Lieutenant*. Princeton, NJ: Princeton University Press, 1996.

##### PERIODICALS:

Waller, Michael J. “State within a State: the KGB and its Successors.” *Perspective* IV,4 (1994).

##### ELECTRONIC:

Federation of American Scientists, FAS Intelligence Resource Program. “Soviet/Russian Intelligence Agencies” <<http://www.fas.org/irp/world/russia/>> (April 18, 2003).

##### SEE ALSO

*Cold War (1945–1950), The start of the Atomic Age*  
*Cold War (1950–1972)*  
*Cold War (1972–1989): The Collapse of the Soviet Union*  
*KGB (Komitet Gosudarstvennoi Bezopasnosti, USSR Committee of State Security)*  
*Russia, Intelligence and Security*  
*Russian Nuclear Materials, Security Issues*

## Space Imaging.

SEE *Satellites, Non-Governmental High Resolution.*

---

## Space Shuttle

---

Although NASA is a civilian space agency, the United States military has used the space shuttle fleet to carry classified military payloads into space. The Department of Defense (DoD) had generally received priority in scheduling national security related flights. In addition to fully classified missions, the Department of Defense (DoD) has contracted shuttle research time and lifted unclassified early warning satellites into orbit. Satellites deployed from

the shuttle, or serviced by shuttle crews, are used for electronic intelligence, photographic and radar reconnaissance, and defense communications.

By 1990, at least eight classified military satellites were placed in orbit during classified shuttle missions. Although the shuttle fleet is still used for a range of classified missions, following the loss of *Challenger* the military shifted emphasis to launching classified military satellites by expendable rockets.

## The Shuttle Program

The space shuttle is a reusable spacecraft that takes off like a rocket, orbits the Earth like a satellite, and then lands like a glider. The space shuttle has been essential to the repair and maintenance of the Hubble Space Telescope and for construction of the International Space Station; it has also been used for a wide variety of other military, scientific, and commercial missions. It is not capable of flight to the Moon or other planets, being designed only to orbit the Earth.

The first shuttle to be launched was the *Columbia*, on April 12, 1981. Since that time, two shuttles have been lost in flight: *Challenger*, which exploded during takeoff on January 28, 1986, and *Columbia*, which broke up during reentry on Feb. 1, 2003. Seven crew members died in each accident. The three remaining shuttles are the *Atlantis*, the *Discovery*, and the *Endeavor*. The first shuttle actually built, the *Enterprise*, was flown in the atmosphere but never equipped for space flight; it is now in the collection of the Smithsonian Museum.

A spacecraft closely resembling the U.S. space shuttle, the Aero-Buran, was launched by the Soviet Union in November, 1988. Buran's computer-piloted first flight was also its last; the program was cut to save money and all copies of the craft that had been built were dismantled.

**Mission of the space shuttle.** At one time, both the United States and the Soviet Union envisioned complex space programs that included space stations orbiting the Earth and reusable shuttle spacecraft to transport people, equipment, raw materials, and finished products to and from these space stations. Because of the high cost of space flight, however, each nation eventually ended up concentrating on only one aspect of this program. The Soviets built and for many years operated space stations (*Salyut*, 1971–1991, and *Mir*, 1986–2001), while Americans have focused their attention on the space shuttle. The brief Soviet excursion into shuttle design (Buran) and the U.S. experiment with Skylab (1973–1979) were the only exceptions to this pattern.

The U.S. shuttle system—which includes the shuttle vehicle itself, launch boosters, and other components—is officially termed the Space Transportation System (STS).

Lacking a space station to which to travel until 1998, when construction of the International Space Station began, the shuttles have for most of their history operated with two major goals: (1) the conduct of scientific experiments in a microgravity environment and (2) the release, capture, repair, and re-release of scientific, commercial, and military satellites. Interplanetary probes such as the Galileo mission to Jupiter (1989–) have been transported to space by the shuttle before launching themselves on interplanetary trajectories with their own rocket systems. Since 1988, the STS has also been essential to the construction and maintenance in orbit of the International Space Station.

One of the most important shuttle missions ever was the repair of the Hubble Space Telescope by the crew of the *Endeavor* in December, 1993 (STS-61). The Hubble had been deployed, by a shuttle mission several years earlier, with a defective mirror; fortunately, it had been designed to be repaired by spacewalking astronauts. The crew of the *Endeavor* latched on to the Hubble with the shuttle's robotic arm, installed a corrective optics package that restored the Hubble to full functionality. The Hubble has since produced a unique wealth of astronomical knowledge.

The STS depends partly on contributions from nations other than the U.S. For example, its Spacelab modules—habitable units, carried in the shuttle's cargo bay, in which astronauts carry out most of their experiments—are designed and built by the European Space Agency, and the extendible arm used to capture and release satellites—the “remote manipulator system” or Canadarm—is constructed in Canada. Nevertheless, the great majority of STS costs continue to be borne by the United States.

**Structure of the STS.** The STS has four main components: (1) the orbiter (i.e., the shuttle itself), (2) the three main engines integral to the orbiter, (3) the external fuel tank that fuels the orbiter's three engines during liftoff, and (4) two solid-fuel rocket boosters also used during liftoff.

**The orbiter.** The orbiter, which is manufactured by Rockwell International, Inc., is approximately the size of a commercial DC-9 jet, with a length of 122 ft (37 m), a wing span of 78 ft (24 m), and a weight of approximately 171,000 lb (77,000 kg). Its interior, apart from the engines and various mechanical and electronic compartments, is subdivided into two main parts: crew cabin and cargo bay.

The crew cabin has two levels. Its upper level—literally “upper” only when the shuttle is in level flight in Earth's atmosphere, as there is no literal “up” and “down” when it is orbiting in free fall—is the flight deck, from which astronauts control the spacecraft during orbit and descent, and its lower level is the crew's personal quarters, which contains personal lockers and sleeping, eating, and toilet facilities. The crew cabin's atmosphere is approximately equivalent to that on the Earth's surface, with a composition 80% nitrogen and 20% oxygen.

The cargo bay is a space 15 ft (4.5 m) wide by 60 ft (18 m) long in which the shuttle's payloads—the modules or satellites that it ports to orbit or back to Earth—are stored. The cargo bay can hold up to about 65,000 lb (30,000 kg) during ascent, and about half that amount during descent.

The shuttle can also carry more habitable space than that in the crew cabin. In 1973, an agreement was reached between the U.S. National Aeronautics and Space Administration (NASA) and the European Space Agency (ESA) for the construction by ESA of a pressurized, habitable workspace that could be carried in the shuttle's cargo bay. This workspace, designated Spacelab, was designed for use as a laboratory in which various science experiments could be conducted. Each of Spacelab module is 13 ft (3.9 m) wide and 8.9 ft (2.7 m) long. Equipment for experiments is arranged in racks along the walls of the Spacelab. The whole module is loaded into the cargo bay of the shuttle prior to take-off, and remains there while the shuttle is in orbit, with the cargo-bay doors opened to give access to space. When necessary, two Spacelab modules can be joined to form a single, larger workspace.

**Propulsion systems.** The power needed to lift a space shuttle into orbit comes from two solid-fuel rockets, each 12 ft (4 m) wide and 149 ft (45.5 m) long, and from the shuttle's three built-in, liquid-fuel engines. The fuel used in the solid rockets is compounded of aluminum powder, ammonium perchlorate, and a special polymer that binds the other ingredients into a rubbery matrix. This mixture is molded into a long prism with a hollow core that resembles an 11-pointed star in cross section. This shape exposes the maximum possible surface area of burning fuel during launch, increasing combustion efficiency.

The two solid-fuel rockets each contain 1.1 million lb (500,000 kg) at ignition, together produce 6.6 million pounds (29.5 million N) of thrust, and burn out only two minutes after the shuttle leaves the launch pad. At solid-engine burnout, the shuttle is at an altitude of 161,000 ft (47,000 m) and 212 miles (452 km) down range of launch site. (In rocketry, "down range" distance is the horizontal distance, as measured on the ground, that a rocket has traveled since launch, as distinct from the greater distance it has traveled along its actual flight path.) At this point, explosive devices detach the solid-fuel rockets from the shuttle's large, external fuel tank. The rockets return to Earth via parachutes, dropping into the Atlantic Ocean at a speed of 55 miles (90 km) per hour. They can then be collected by ships, returned to their manufacturer (Morton Thiokol Corp.), refurbished and refilled with solid fuel, and used again in a later shuttle launch.

The three liquid-fuel engines built into the shuttle itself have been described as the most efficient engines ever built; at maximum thrust, they achieve 99% combustion efficiency. (This number describes combustion efficiency, not end-use efficiency. As dictated by the laws of physics, less than half of the energy released in combustion can be communicated to the shuttle as kinetic energy,

even by an ideal rocket motor.) The shuttle's main engines are fueled by liquid hydrogen and liquid oxygen stored in the external fuel tank (built by Martin Marietta Corp.), which is 27.5 ft (8.4 m) wide and 154 ft (46.2 m) long. The tank itself is actually two tanks—one for liquid oxygen and the other for liquid hydrogen—covered by a single, aerodynamic sheath. The tank is kept cold (below -454°F [-270°C]) to keep its hydrogen and oxygen in their liquid state, and is covered with an insulating layer of stiff foam to keep its contents cold. Liquid hydrogen and liquid oxygen are pumped into the shuttle's three engines through lines 17in (43 cm) in diameter that carry 1,035 gal (3,900 l) of fuel per second. Upon ignition, each of the liquid-fueled engines develops 367,000 lb (1.67 million N) of thrust.

The three main engines turn off at approximately 522 seconds, when the shuttle has reached an altitude of 50 miles (105 km) and is 670 miles (1,426 km) down range of the launch site. At this point, the external fuel tank is also jettisoned. Its fall into the sea is not controlled, however, and it is not recoverable for future use.

Final orbit is achieved by means of two small engines, the Orbital Maneuvering System (OMS) engines located on external pods at the rear of the orbiter's fuselage. The OMS engines are fired first to insert the orbiter into an elliptical orbit with an apogee (highest altitude) of 139 miles (296 km) and a perigee (lowest altitude) of 46 miles (98 km). They are fired again to nudge the shuttle into a final, circular orbit with a radius of 139 miles (296 km). All these figures may vary slightly from mission to mission.

**Orbital maneuvers.** For making fine adjustments, the spacecraft depends on six small rockets termed vernier jets, two in the nose and four in the OMS pods. These allow small changes in the shuttle's flight path and orientation.

The computer system used aboard the shuttle, which governs all events during takeoff and on which the shuttle's pilots are completely dependent for interacting with its complex control surfaces during the glide back to Earth, is highly redundant. Five identical computers are used, four networked with each other using one computer program, and a fifth operating independently. The four linked computers constantly communicate with each other, testing each other's decisions and deciding when any one (or two or three) are not performing properly and eliminating that computer or computers from the decision-making process. In case all four of the interlinked computers malfunction, decision-making would be turned over automatically to the fifth computer.

This kind of redundancy is built into many essential features of the shuttle. For example, three independent hydraulic systems are available, each with an independent power systems. The failure of one or even two systems does not, therefore, place the shuttle in what its engineers would call a "critical failure mode"—that is,

cause its destruction. Many other components, of course, simply cannot be built redundantly. The failure of a solid-fuel rocket booster during liftoff (as occurred during the *Challenger* mission of 1981) or of the delicate tiles that protect the shuttle from the high temperatures of atmospheric reentry (as occurred during the *Columbia* mission of 2003) can lead to loss of the spacecraft.

**Descent.** Some of the most difficult design problems faced by shuttle engineers were those involving the reentry process. When the spacecraft has completed its mission in space and is ready to leave orbit, its OMS fires just long enough to slow the shuttle by 200 MPH (320 km/h). This modest change in speed is enough to cause the shuttle to drop out of its orbit and begin its descent to Earth.

When the shuttle reaches the upper atmosphere, significant amounts of atmospheric gases are first encountered. Friction between the shuttle—now traveling at 17,500 MPH (28,000 km/h)—and air molecules causes the spacecraft's outer surface to heat. Eventually, portions of the shuttle's surface reach 3,000°F (1,650°C).

Most materials normally used in aircraft construction would melt or vaporize at these temperatures. It was necessary, therefore, to find a way of protecting the shuttle's interior from this searing heat. NASA decided to use a variety of insulating materials on the shuttle's outer skin. Parts less severely heated during reentry are covered with 2,300 flexible quilts of a silica-glass composite. The more sensitive belly of the shuttle is covered with 25,000 porous insulating tiles, each approximately 6 in (15 cm) square and 5 in (12 cm) thick, made of a silica-borosilicate glass composite.

The portions of the shuttle most severely stressed by heat—the nose and the leading edges of the wings—are coated with an even more resistant material termed carbon-carbon. Carbon-carbon is made by attaching a carbon-fiber cloth to the body of the shuttle and then baking it to convert it to a pure carbon substance. The carbon-carbon is then coated to prevent oxidation (combustion) of the material during descent.

**Landing.** Once the shuttle reaches the atmosphere, it ceases to operate as a spacecraft and begins to function as a glider. Its flight during descent is entirely unpowered; its movements are controlled by its tail rudder, a large flap beneath the main engines, and elevons (small flaps on its wings). These surfaces allow the shuttle to navigate at forward speeds of thousands of miles per hour while dropping vertically at a rate of some 140 MPH (225 km/h). When the aircraft finally touches down, it is traveling at a speed of about 190 knots (100 m per second), and requires about 1.5 miles (2.5 km) to come to a stop. Shuttles can land at extra-long landing strips at either Edwards Air Force Base in California or the Kennedy Space Center in Florida.

**Military shuttle missions and the military spaceplane.** Many shuttle missions have been partly or entirely military in nature. Eight military missions—the majority—have been devoted to the deployment of secret military satellites in three categories: signals intelligence (i.e., eavesdropping on radio communications), optical and radar reconnaissance of the Earth, and military communications. All these deployments occurred between 1982 and 1990, after which the military chose to use uncrewed launch rockets for all classified missions. The shuttle has also supported several military experimental missions and nonclassified satellite deployments. One such was the *Discovery* mission (STS-39) launched on April 28, 1991 (STS-39), which carried multi-experiment hardware platforms designed to be released into space then retrieved by the shuttle after having recorded various observations of space conditions. All science aboard STS-39 was related to the Strategic Defense Initiative.

The U.S. military is developing an armed space shuttle system or "military spaceplane" of its own, and says that it intends to deploy such a system by 2012. According to an Air Force status report released in January 2002, "a military spaceplane armed with a variety of weapons payloads (e.g. unitary penetrator, small diameter bombs, etc.) will be able to precisely attack and destroy a considerable number of critical targets while satisfying the requirement for precise weapons (i.e. circular error probable [CEP] of less than or equal to three meters)... Spaceplanes can support a wide range of military missions including a worldwide precision strike capability; rapid unpredictable reconnaissance; new space control and missile defense capabilities; and both conventional and new tactical spacelift missions that enable augmentation and reconstitution of space assets." The military spaceplane would also enable the military to deploy satellites on short notice. The Air Force envisions a fleet of some 10 spaceplanes stationed in the continental United States as one component of a "Global Strike Task Force" that, it says, will be "capable of striking any target in the world within 24 hours."

**The *Challenger* disaster.** Disasters have been associated with both the Soviet (now Russian) and American space programs. The first of the two disasters suffered by the shuttle program took place on January 28, 1986, when the external fuel tank of the shuttle *Challenger* exploded only 73 seconds into the flight. All seven astronauts were killed, including high-school teacher Christa McAuliffe, who was flying on the shuttle as part of NASA's public-relations campaign "Teachers in Space," designed to bolster young people's interest in human space flight.

The *Challenger* disaster prompted a comprehensive study to discover its causes. On June 6, 1986, the Presidential Commission appointed to analyze the disaster published its report. The reason for the disaster, said the

commission, was the failure of an O-ring (literally, a flexible O-shaped ring or gasket) in a joint connecting two sections of one of the solid rocket engines. The O-ring ruptured, allowing flames from the rocket's interior to jet out, burning into the external fuel tank and causing it to explode.

As a result of the *Challenger* disaster, many design changes were made. Most of these (254 modifications in all) were made in the orbiter. Another 30 were made in the solid rocket booster, 13 in the external tank, and 24 in the shuttle's main engine. In addition, an escape system was developed that would allow crew members to abandon a shuttle via parachute in case of emergency, and NASA redesigned its launch-abort procedures. Also, NASA was instructed by Congress to reassess its ability to carry out the ambitious program of shuttle launches that it had been planning. The military began reviving its non-shuttle launch options and switched fully to its own boosters for classified satellite launches after 1990.

The STS was essentially shut down for a period of 975 days while NASA carried out the necessary changes and tested its new systems. On September 29, 1988, the first post-*Challenger* mission was launched, STS-26. On that flight, *Discovery* carried NASA's TDRS-C communications satellite into orbit, putting the American STS program back on track once more.

**The *Columbia* disaster.** Scores of shuttle missions were successfully carried out between the *Challenger's* successful 1988 mission and February 1, 2003, when disaster struck again. The space shuttle *Columbia* broke up suddenly during re-entry, strewing debris over much of Texas and several other states and killing all seven astronauts on board. At the time of this writing, analysts speculate that the most likely cause of the loss of the spacecraft related to some form of damage to the outer protective layer of heat-resistant tiles or seals that protect the shuttle's interior from the 3,000°F (1,650°C) plasma (superheated gas) that envelops it during reentry. As described earlier, a coating of rigid foam insulation is used to keep the external fuel tank cool; video cameras recording the *Columbia's* takeoff show that a piece of this foam broke off 80 seconds into the flight and burst against the shuttle's wing at some 510 MPH (821 km/h). Pieces of foam have broken off and struck shuttles during takeoff before, but this was the largest piece ever—at least 2.7 lb (1.2 kg) and the size of a briefcase.

While *Columbia* was in orbit, NASA engineers, who were aware that the foam strike had occurred, analyzed the possibility that it might have caused significant damage to the shuttle, but decided that it could not have: computer simulations seemed to show that the brittle tiles covering the shuttle's essential surfaces would not be severely damaged. In any event, there were no contingency procedures to fix any such damage. The shuttle does not carry spare tiles or means to attach them, nor does it carry gear that would make a spacewalk to the bottom of the shuttle feasible.

NASA officials also insisted that it would not have been possible to fly the shuttle in such a way as to spare the damage surfaces, as the shuttle's path is already designed to minimize heating on reentry.

Regardless of the exact reason, the shuttle's skin was breached, whether by mechanical damage or some other cause, and hot gases formed a jet that caused considerable damage to the left wing from inside. During reentry, the wing began to break up, experiencing greatly increased drag. The autopilot struggled to compensate by firing steering rockets, but could only stabilize the shuttle temporarily.

As this book goes to press, the loss of the *Columbia* has, like the loss of the *Challenger* in 1986, put a temporary stop to shuttle launches. A moratorium on shuttle launches will also have an impact on the International Space Station, which depends on the shuttle to bring it the fuel it needs to stay in orbit and which cannot be completed without components that only the space shuttle can carry. In the wake of the *Columbia* disaster, NASA and other governmental officials worked with an independent panel's review of the accident and sought technical improvements to the STS program that might prevent future problems while, at the same time returning the remaining shuttles to flight status as soon as safely possible.

#### ■ FURTHER READING:

##### BOOKS:

- Barrett, Norman S. *Space Shuttle*. New York: Franklin Watts, 1985.
- Curtis, Anthony R. *Space Almanac*. Woodboro, MD: Arcsoft Publishers, 1990.
- Dwiggins, Don. *Flying the Space Shuttles*. New York: Dodd, Mead, 1985.

##### PERIODICALS:

- Barstow, David. "After Liftoff, Uncertainty and Guesswork." *New York Times*. (February 17, 2003).
- Broad, William J. "Outside Space Experts Focusing on Blow to Shuttle Wing." *New York Times*. (February 15, 2003).
- Chang, Kenneth. "Columbia Was Beyond Any Help, Officials Say." *New York Times*. (February 4, 2003).
- . "Disagreement Emerges over Foam on Shuttle Tank." *New York Times*. (February 21, 2003).
- Seltzer, Richard J. "Faulty Joint behind Space Shuttle Disaster." *Chemical & Engineering News* (23 June 1986): 9–15.

##### ELECTRONIC:

- Space and Missile Systems Center (SMC), United States Air Force. "The Military Space Plane: Providing Transformational and Responsive Global Precision Striking Power." Jan. 17, 2002. <<http://www.spaceref.com/news/viewsr.html?pid=4523>> (Feb. 17, 2003).

## SEE ALSO

*NASA (National Air and Space Administration) Near Space Environment Satellites, Non-Governmental High Resolution Satellites, Spy*

## Spain, Intelligence and Security

Spain is one of the few Western countries in which a single agency handles both internal and external intelligence. This is CNI, or Centro Nacional de Inteligencia (National Intelligence Center). In addition to CNI, the Spanish military and interior ministry each have their own intelligence branches, whose work includes monitoring Basque terrorists.

**CNI.** From the end of the Spanish Civil War in 1939 until 1975, Spain was under the right-wing dictatorship of Generalissimo Francisco Franco. Following Franco's death, the country liberalized rapidly, and in 1977 it dissolved the old intelligence services that Franco had used to maintain control of the country. In place of the Franco-era Political-Social Brigade, the Spanish government established the Centro Superior de Informacion de la Defensa (CESID or Higher Defense Intelligence Center). CESID in 2001 became CNI.

Nominally a civilian agency, though headed by military personnel, CESID placed a priority on monitoring both the homeland and outlying territories, including the Spanish-owned enclaves of Ceuta and Melilla on the Moroccan coast. It also maintained close relations not only with the intelligence services of Arab countries in North Africa and the Middle East, but with Israel's Mossad as well.

**Ministry of Interior.** Whereas CNI is primarily concerned with intelligence, the principal focus of the interior ministry is security. The Ministry of Interior is divided into three groups: the National Police, who conduct investigations nationwide and maintain security in urban areas; the Civil Guard, which patrols rural areas, borders, and highways; and autonomous police forces, which have replaced the Civil Guard in Galicia, Catalonia, and the Basque Country.

The last of these regions was the site of the greatest threat to domestic security, in the form of ETA (Euzkadi Ta Azkatasuna or Basque Homeland and Liberty), the separatist organization that claimed to represent the Basque people of northwestern Spain. A right-wing force known

as GAL (Grupo Antiterrorista de Liberacion or Antiterrorist Liberation Group), believed by some observers to be composed of Civil Guard members, conducted reprisals against ETA.

In May 2002, Spain's parliament passed a law to create an intelligence and security coordinating committee which would oversee the activities of CNI, the police, and the national guard.

### ■ FURTHER READING:

#### BOOKS:

Bennett, Richard M. *Espionage: An Encyclopedia of Spies and Secrets*. London: Virgin Books, 2002.

#### PERIODICALS:

Champion, Marc. "How Do Other Countries Coordinate Security?" *Wall Street Journal*. (June 12, 2002): A14.

#### ELECTRONIC:

Spain—Intelligence Agencies. Federation of American Scientists. <<http://www.fas.org/irp/world/spain/index.html>> (March 1, 2003).

### SEE ALSO

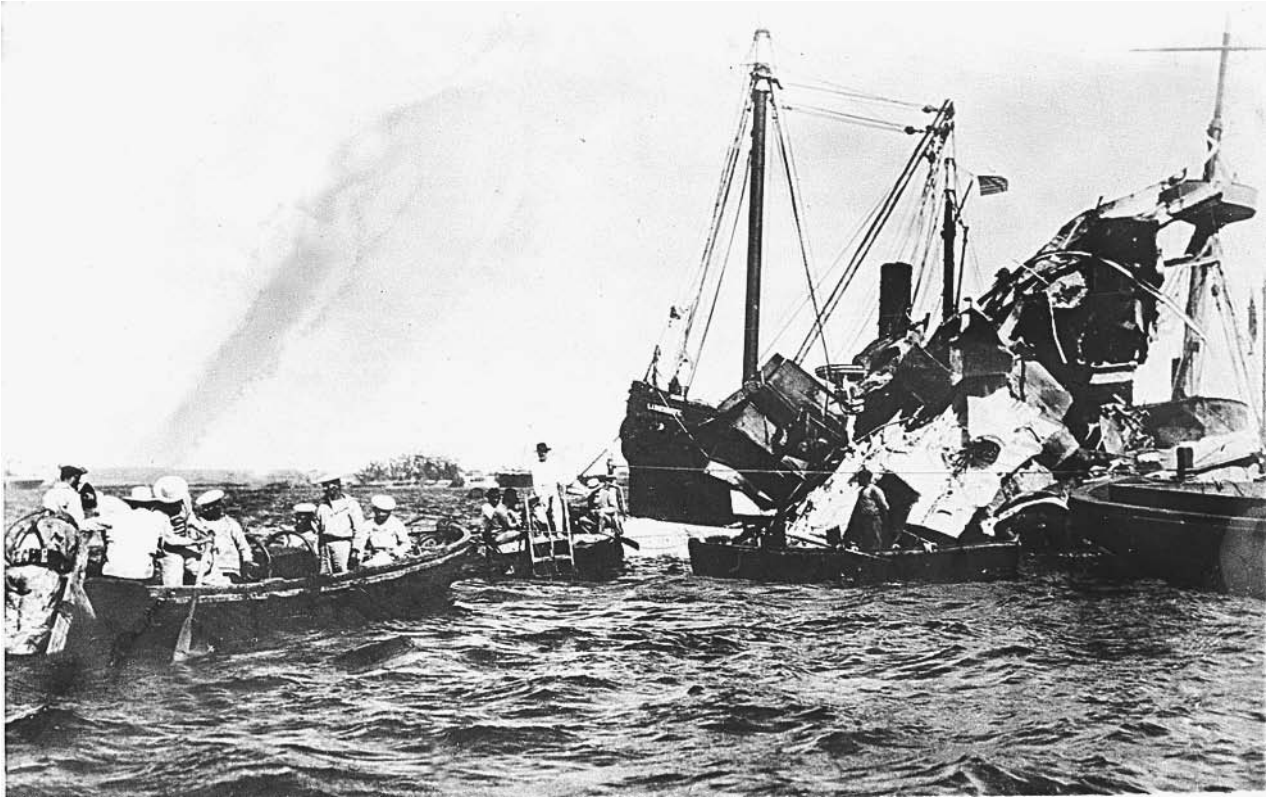
*Italy, Intelligence and Security*  
*Morocco, Intelligence and Security*  
*Spanish-American War*

## Spanish-American War

### ■ ADRIENNE WILMOTH LERNER

In the late nineteenth century, the United States grew in industrial and economic strength. By the 1880s, the nation was one of the most robust in the Western Hemisphere, wielding increasing power in the region despite a stated policy of neutrality. In 1898, diplomatic relations between the United States and Spain began to sour over Spain's domination of Latin America and some parts of the Caribbean. Reports of the brutal rule of Spanish General Valeriano Wyler in Cuba inflamed public opinion in the United States. The convergence of anti-Spanish public opinion and the government's desire to protect American economic interests in Cuba prompted tense diplomatic meetings between Spain and the United States.

During the negotiations, two events spurred the United States to declare war. A U.S. ship, the USS *Maine* sank off the coast of Cuba on February 15, 1898. A Navy inquiry board incorrectly declared that a mine fatally wounded the



Lifeboats rescue surviving crewmen of the wrecked USS *Maine* anchored in Havana, Cuba, after an explosion destroyed the battleship in 1898, serving as the catalyst for the outbreak of the Spanish-American War. AP/WIDE WORLD PHOTOS.

vessel. 266 Navy seamen and two high-ranking officers perished in the accident. The event consumed newspaper headlines for weeks. Sensationalistic reporting, dubbed “yellow journalism,” helped to swell the tide of pro-war sentiment in the United States.

Within weeks of the sinking of the *Maine*, intelligence operatives intercepted a private letter between the Spanish Ambassador to the United States and a friend in Havana, Cuba. The letter disparaged U.S. President McKinley, and hinted at plans to commit acts of sabotage against American property in Cuba. The letter was published by several newspapers, further agitating public opinion. On April 19, 1898, Congress resolved to end Spanish rule in Cuba.

In the first military action of the war, the United States blockaded Cuban ports on April 22, 1898. The Navy transferred several vessels to neighboring Florida to consolidate the forces available to fight the Spanish in the Caribbean. Naval presence off the Florida coast also facilitated the transfer of information from the battlefield to the government in Washington, D.C.

The Office of Naval Intelligence established sophisticated communications intelligence operations in support of their efforts in Cuba. Martin Hellings, who worked for the International Ocean Telegraph Company, was sent to Key West, Florida, to intercept Spanish messages. Hellings

convinced other telegraph operators to copy Spanish diplomatic messages and deliver the copies to him. Within a few days, he operated a sizable communications ring, conducting surveillance on underwater and land-based telegraph cables. Hellings also employed a courier to run special messages between his offices and United States ships in the region.

The theater of war rapidly expanded to include other Spanish strongholds, including the Philippines. Intelligence operations were not initially as well developed in the Pacific as they were in the region around Cuba. Cuba’s proximity to the Florida coast aided intelligence and espionage operations. United States military commanders knew little about the Philippines and the Spanish defenses there. To obtain information, the Office of Navy Intelligence and the Army’s Military Intelligence Division employed human intelligence. Agents were sent to the remote islands to obtain information about Spanish defenses, military strength, and island terrain. The operation moved swiftly, and within weeks, United States commanders learned that the Spanish were ill-prepared to fight a strong offensive in the Philippines.

On May 1, 1898, the United States Asiatic Squadron, under the command of George Dewey, sailed into Manila Bay and attacked the Spanish. The Spanish fleet was decimated, but the United States sustained no losses.

Though the Spanish surrendered the Philippines, the United States fleet remained, and began a campaign to take the island as a United States territory. The ensuing conflict lasted until 1914.

Human intelligence was not limited to operations in the Philippines. The United States employed covert agents in Europe, Cuba, and Canada. These agents aided the war effort by spying on Spanish diplomats abroad and providing intelligence information to dissident groups in Cuba. German-educated Henry Ward traveled to Spain in the guise of a German physician. William Sims, an American attaché in Paris, managed a spy ring throughout the Mediterranean. In Cuba, Andrew Rowan united rebel groups and reported on the location and size of the Spanish fleet. He supervised the trafficking of arms to rebel outfits and helped plan their assaults on Spanish targets. Human intelligence also contributed to counterintelligence efforts. Based on agent reports, the United States Secret Service was able to infiltrate and destroy a Spanish spy ring working in Montreal, Canada.

In June 1898 United States intelligence learned, via telegraph intercepts, that the Spanish fleet planned to attack the U.S. blockade in Cuba and draw ships into a naval battle in the Caribbean. When the Spanish fleet arrived in the region, United States Naval Intelligence tracked them and gave chase. United States commanders hoped to deplete Spanish fuel reserves before engaging them in battle. The United States backed off, and redeployed to aid blockade ships stationed around Havana. The Spanish ships proceeded undetected to the narrow harbor of Santiago, Cuba. When the Spanish commander telegraphed his government to declare his position, U.S. agents working in Florida intercepted the cable. The United States fleet moved to intercept the Spanish at Santiago. The U.S. Navy blockaded the port and immobilized the Spanish fleet. The Spanish attempted to run the blockade on July 3, but the entire fleet of six ships was destroyed.

In the final phase of the war, the United States deployed ground forces to sweep Spanish forces out of Havana and Santiago. The “Rough Riders,” the most famous of which was Theodore Roosevelt, worked with rebel groups to take control of the nation’s capitol and ferret out remaining Spanish forces in the countryside. The U.S. troops then departed Cuba for Puerto Rico, driving the Spanish from the island.

The war ended with the Spanish surrender on July 17, 1898. The event signaled a new international stance for the United States, as the nation began to acquire territories and dominate the politics of the Western Hemisphere. As a result of the Spanish-American War, or in its immediate wake, the United States gained Guantanamo Bay, Puerto Rico, Guam, and Hawaii.

The Spanish-American War, though a brief conflict, helped to revolutionize United States intelligence organizations and their operations. Before the war, agencies like the Office of Naval Intelligence relied on openly available

sources for their information. After the war, personnel were trained in espionage tradecraft, and covert operations became standard intelligence community practice. Congress briefly entertained the idea of establishing a permanent, civilian intelligence corps, but the agency never materialized. Despite the progress made with technological surveillance, espionage tradecraft, and inter-agency cooperation made during the war, the intelligence community was once again allowed to slip into disarray until the eve of World War I.

#### ■ FURTHER READING:

##### BOOKS:

Musicant, Ivan. *Empire by Default: The Spanish-American War and the Dawn of the American Century*. Henry Holt, 1998.

O’Toole, G. J. A. *The Spanish-American War: An American Epic, 1898*. New York: W.W. Norton, 1986.

##### SEE ALSO

*Monroe Doctrine*

---

## Special Collection Service, United States

---

The National Security Agency (NSA) has a reputation as the most secretive major component of the United States intelligence community, but it is a veritable open book in comparison to one of its subsidiary organizations, the Special Collection Service (SCS). The latter is known to be engaged in communications intelligence (COMINT), primarily in hostile countries, and its personnel appears to include both NSA and Central Intelligence Agency (CIA) operatives.

So secretive that it is sometimes jokingly called “No Such Agency,” NSA is home to an even more obscure group, the Central Security Service (CSS). Established in 1972 to provide information security to U.S. communications and crack other nations’ codes and ciphers, CSS has within it—like a nesting matryoshka doll—the still more elite and clandestine SCS. Composed primarily of NSA specialists, SCS operatives typically use diplomatic cover in order to put in place eavesdropping equipment in areas where access to U.S. intelligence by less laborious means would be considerably more difficult.

In 1999, one United Nations Special Commission (UNSCOM) weapons inspector claimed that SCS had installed in-country radio relays for UNSCOM that greatly



extended U.S. listening capabilities in Iraq. One of the few references to SCS by federal government sources was the affidavit in the 2001 case of accused spy Robert Hanssen, who was alleged to have provided the Russians with information about the organization.

■ FURTHER READING:

BOOKS:

Bamford, James. *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency: From the Cold War through the Dawn of a New Century*. New York: Doubleday, 2001.

Polmar, Norman, and Thomas B. Allen. *Spy Book: The Encyclopedia of Espionage*. New York: Random House, 1998.

ELECTRONIC:

National Security Agency. <<http://www.nsa.gov/>> (March 24, 2003).

Special Collection Service. Federation of American Scientists. <<http://www.fas.org/irp/agency/scs/>> (April 2, 2003).

SEE ALSO

*COMINT (Communications Intelligence)*

*Echelon*

*Information Warfare*

*NSA (United States National Security Agency)*

*Satellites, Spy*

*SIGINT (Signals Intelligence)*



Transportation Undersecretary John Magaw speaks during a press conference at the Federal Aviation Administration in Washington, where he discussed an agreement to better protect aviation safety agency whistleblowers against reprisals in the era of terrorist threats. AP/WIDE WORLD PHOTOS.

## Special Counsel and Security Related "Whistleblower" Protection Issues, United States Office

■ JUDSON KNIGHT

In 1989, the United States Congress passed the Whistleblower Protection Act, which provided protections for federal employees who reported wrongdoing, including theft and fraud, in the workplace. Since that time, several high-profile cases have involved personnel claiming protection through the Office of Special Counsel (OSC), established by that Act. Several federal intelligence agencies, however, are exempt from the whistleblower statute. As a result of reorganizations in airport security following the September 2001, terrorist attacks, whistleblower protections also do not extend to some airport personnel.

**Whistleblower provisions.** Acts of malfeasance reported to the OSC Disclosure Unit (DU) fall into five general categories: violations of laws, rules, or regulations; gross mismanagement; waste of funds; abuse of authority; and specific danger to public health and safety. The

Whistleblower Protection Act (5 U.S.C. 1213) put in place a system unique among existing governmental whistleblower measures. Provisions of the Act protected the confidentiality of the whistleblower, gave the OSC authority to direct an agency head to investigate charges, and compelled the OSC to provide reports on all whistleblower investigations to the president and the appropriate congressional committees.

The statute had several caveats, however. Among these was a provision whereby, if the Special Counsel determined that it was necessary to do so, the identity of the whistleblower could be disclosed without his or her consent. Additionally, the law exempted the Federal Bureau of Investigation (FBI), Central Intelligence Agency, and National Security Agency from whistleblower investigations.

**The whistleblower statute in practice.** A law accompanying the whistleblower statute required the president to establish a separate system to protect FBI whistleblowers, and

after a lawsuit filed by the FBI's Frederic Whitehurst in April 1997, President William J. Clinton instructed Attorney General Janet Reno to create such a system. Eighteen months later, no such system was in place, prompting a lawsuit against the federal government by several FBI employees. Among these was Cheryl Whitehurst, who claimed that she had been the target of harassment due to the whistleblowing report of her husband, a respected explosives residue analyst who charged wrongdoing at the laboratory where he worked.

Other notable whistleblower cases have involved Immigration and Naturalization Service official Neil Jacobs in 1998, Centers for Disease Control branch chief William C. Reeves in 1999, and Army Corps of Engineers economist Donald C. Sweeney II in 2000. In contrast to these federal employees, whose whistleblower rights were never in question, federal airport baggage screeners are not covered by the whistleblower statute.

After consultation with the OSC, the newly created Transportation Security Administration (TSA) determined that a whistleblower action could shut down security operations at an airport, creating an unacceptable situation for an already overtaxed air transportation infrastructure. The law creating the TSA, passed by Congress in November 2001, had given its director broad authority for hiring and firing, and in February 2002, TSA chief John W. Magaw elected to use this power to exempt a portion of his agency from the whistleblower statute.

#### ■ FURTHER READING:

##### PERIODICALS:

- Barr, Stephen. "Probe's Findings Support INS Whistleblower." *Washington Post*. (December 16, 1998): A29.
- Grunwald, Michael. "Former FBI Workers File Whistleblower Suit." *Washington Post*. (October 20, 1998): A17.
- . "Agency Says Engineers Likely Broke Rules." *Washington Post*. (February 29, 2000): A4.
- Schneider, Greg. "No Whistleblowing Protections for Airport Baggage Screeners." *Washington Post*. (February 8, 2002): A29.
- Stephens, Joe, and Valerie Strauss. "Retaliation Alleged at CDC; Scientist Disclosed Diversion of Funds." *Washington Post*. (August 6, 1999): A19.

##### ELECTRONIC:

Whistleblower Disclosures. U.S. Office of Special Counsel. <<http://www.osc.gov/wbdisc.htm>> (April 2, 2003).

##### SEE ALSO

*Airline Security*  
*Civil Aviation Security, United States*  
*FBI (United States Federal Bureau of Investigation)*  
*Intelligence, United States Congressional Oversight*

*President of the United States (Executive Command and control of Intelligence Agencies)*

## Special Operations Command, United States

Special operations forces (SOFs) are elite units of the United States military services that are used for purposes that include counterterrorism, asymmetric warfare, forward reconnaissance, and preparation for landing by airborne and conventional troops in a combat zone. Though some such units have existed since World War II, the formal organization of special operations did not emerge until much later, culminating in the establishment of the U.S. Special Operations Command (SOCOM) on April 16, 1987. Headquartered at MacDill Air Force Base in Florida, SOCOM brings together special operations units and closely related support groups, including psychological warfare contingents, under a single unified command.

SOCOM is one of the nine unified commands of the U.S. Department of Defense (DOD), and its commander-in-chief (USCINCSOC), a four-star general, is the only unified command leader with authority to make purchases in support of his troops. The SOCOM budget for fiscal year 2002 was \$4.9 billion, well over 1 percent of DoD appropriations. In September 2002, after Defense Secretary Donald Rumsfeld called for increased SOF involvement in the war on terror, USCINCSOC General Charles Holland presented him with a five-year budget that would double funding for SOCOM.

Components of SOCOM include the U.S. Army Special Operations Command, Joint Special Operations Command, and John F. Kennedy Special Warfare Center and School, all located at Fort Bragg, North Carolina; the Air Force Special Operations Command and Special Operations School at Hurlburt Field, Florida; and the Naval Special Warfare Command and Special Warfare Center at Coronado, California. Among the many elite units that make up SOCOM are the U.S. Army Rangers, Special Forces ("Green Berets"), and Delta Force; the Navy SEALs (sea, air, land); and various Air Force special operations groups.

#### ■ FURTHER READING:

##### BOOKS:

- Bohrer, David. *America's Special Forces*. St. Paul, MN: MBI Publishing, 2002.
- Clancy, Tom, and John Gresham. *Special Forces: A Guided Tour of U.S. Army Special Forces*. New York: Berkley Books, 2001.

Clancy, Tom, Tony Koltz, and Carl Stiner. *Shadow Warriors: Inside the Special Forces*. New York: G.P. Putnam's Sons, 2002.

#### PERIODICALS:

Wall, Robert. "Conflict Could Test Special Ops Improvements." *Aviation Week & Space Technology* 155, no. 14 (October 1, 2001): 30–31.

#### ELECTRONIC:

Special Operations.com. <<http://www.specialoperations.com/>> (April 2, 2003).

U.S. Air Force Special Operations Command. <<http://www.afsoc.af.mil/>> (April 2, 2003).

U.S. Army Special Operations Command. <<http://www.soc.mil/>> (April 2, 2003).

U.S. Army Special Operations Command. <[http://www.bragg.army.mil/18abn/usa\\_special\\_operations\\_command.htm](http://www.bragg.army.mil/18abn/usa_special_operations_command.htm)> (April 2, 2003).

#### SEE ALSO

*Asymmetric Warfare*

*Delta Force*

*DoD (United States Department of Defense)*

*Guerilla Warfare*

*SEAL Teams*

*United States, Counter-terrorism Policy*

## Special Relationship: Technology Sharing between the Intelligence Agencies of the United States and United Kingdom

■ JUDSON KNIGHT

During World War II, the intelligence services of the United States and the United Kingdom worked together in their efforts against the Axis powers, particularly in Europe, and formalized the collaboration with agreements in 1943 and 1946. Only in the postwar era did the United States emerge as the dominant partner, and even then, many of the most important technological advances in intelligence came from Britain. Among the most visible examples of U.S.-British cooperation in the early twenty-first century were joint military efforts in Afghanistan and Iraq. Behind these undertakings lay a more extensive framework of cooperation in intelligence, whose most significant known component is the Echelon global surveillance system.

**U.S. and British relations through 1945.** Great Britain is one of the only nations, other than Germany, against which Americans have fought twice: first in the Revolutionary War (1775–83), and later in the War of 1812. A century later, the two nations allied against the Central Powers in World War I. The "special relationship" between the Anglo-American powers only became apparent in World War II, when Italy and Russia signed pacts with the Nazis, and France readily capitulated to them. With Britain the only European nation opposing Hitler, the United States—which did not enter the war until two years after it began in Europe—transferred considerable war materiel to the United Kingdom through the Lend-Lease program.

At that time, Britain, with its vast empire, was still perceived as the greater of the two powers, and in many regards, it maintained the lead. Despite the legendary status that wartime U.S. intelligence efforts have gained in retrospect, it was the British who scored the single greatest intelligence breakthrough of the war: Ultra, the successful effort to decipher German radio transmissions made with the Enigma machine. This in turn gave the Allies an enormous advantage over the Germans, who only learned—along with the rest of the world—about Ultra long after the war was over.

Certainly the Soviets did not know about Ultra, or any number of other secrets maintained by the democratic portion of the allied force. In a stroke of good fortune for the postwar world, the instincts of the anticommunist British prime minister, Winston Churchill, prevailed over the desire of U.S. president Franklin D. Roosevelt to share information equitably, and the two countries withheld the most sensitive information from the Soviets. Dictator Josef Stalin did not even know about plans for the Normandy invasion almost until the launch of the attack in June 1944.

**Formal agreements and technology-sharing.** Midway of the war, the United States and United Kingdom formalized their special relationship with the British-United States Agreement (Brusa) of May 17, 1943. Brusa put into writing what had already existed in fact: virtually complete sharing of signals intelligence. As members of the British Empire, Australia and Canada—which also participated in the Normandy invasion—later also signed on to the agreement.

These four nations, along with New Zealand, became parties to the United Kingdom-United States of America Security Agreement, known as UKUSA, signed on March 5, 1946. UKUSA greatly extended the provisions of Brusa, allowing for standardized terminology, techniques, and procedures. After 1947, the U.S. National Security Agency took the lead in UKUSA, around which grew the vast intelligence-gathering network known as Echelon. Only in the late 1990s did Echelon become public knowledge.

Throughout much of the period before and during World War II, and for several decades thereafter, Great

Britain played a powerful role in the technological dimension of this arrangement. The British had, if not the lead, at least a position of parity with the Americans where technological advances were concerned. Particularly notable were the many advances they made in the technology of naval warfare, both for aircraft carriers and the planes associated with them. One outstanding example of this is the British Harrier jet, whose unusual ability to hover made it an ideal craft for the U.S. Marines.

**America's closest friend.** In the years since Vietnam, as anti-Americanism took hold in much of western Europe and the developing world, Britain distinguished itself by its virtually unflinching support for the United States. This became particularly apparent following the September 11, 2001, terrorist attacks on the United States. The United Kingdom made this support concrete, first in the war against the Taliban regime in Afghanistan, and later against Saddam Hussein's dictatorship in Iraq. (Australia, too, supported the United States with troops in both efforts, while Canada provided troops for the Afghanistan war.) At the same time, British technological advances remained a vital aspect of the partnership: in October 2002, for instance, the U.S. General Services Administration awarded a contract to British software developer Autonomy for a system to be used in tracking suspected terrorists.

#### ■ FURTHER READING:

Aldrich, Richard J. *Intelligence and the War against Japan: Britain, America, and the Politics of Secret Service*. New York: Cambridge University Press, 2000.

———. *The Hidden Hand: Britain, America, and Cold War Secret Intelligence*. Woodstock, NY: Overlook Press, 2002.

Richelson, Jeffrey. *The Ties that Bind: Intelligence Cooperation between the UKUSA Countries*. Boston: Unwin Hyman, 1990.

Whiting, Charles. *The Spymasters: The True Story of Anglo-American Intelligence Operations within Nazi Germany, 1939–1945*. New York: Saturday Review Press, 1976.

#### PERIODICALS:

Chapman, Gary. "U.S.-British Cyber-Spy System Puts European Countries on Edge." *Los Angeles Times*. (August 16, 1999): 3.

Markoff, John. "British Concern to Help U.S. Track Terrorists." *New York Times*. (October 12, 2002): A8.

#### SEE ALSO

*Aircraft Carrier*  
*Enduring Freedom, Operation*  
*Enigma*  
*Iraqi Freedom, Operation (2003 War Against Iraq)*  
*United Kingdom, Intelligence and Security*

## Spectroscopy

■ JULI BERWALD

Spectroscopy is the measurement of the absorption, scattering, or emission of electromagnetic radiation by atoms or molecules. Absorption is the transfer of electromagnetic energy from a source to an atom or molecule. Scattering is the redirection of light as a result of its interaction with matter. Emission is the transition of electromagnetic energy from a one energy level to another energy level that results in the emission of a photon.

When atoms or molecules absorb electromagnetic energy, the incoming energy transfers the quantized atomic or molecular system to a higher energy level. Electrons are promoted to higher orbitals by ultraviolet or visible light; vibrations are excited by infrared light, and rotations are excited by microwaves. Atomic-absorption spectroscopy measures the concentration of an element in a sample, whereas atomic-emission spectroscopy aims at measuring the concentration of elements in samples. UV-VIS absorption spectroscopy is used to obtain qualitative information from the electronic absorption spectrum, or to measure the concentration of an analyte molecule in solution. Molecular fluorescence spectroscopy is a technique for obtaining qualitative information from the electronic fluorescence spectrum, or for measuring the concentration of an analyte in solution.

Infrared spectroscopy has been widely used in the study of surfaces. The most frequently used portion of the infrared spectrum is the region where molecular vibrational frequencies occur. This technique was first applied around the turn of the twentieth century in an attempt to distinguish water of crystallization from water of constitution in solids.

Ultraviolet spectroscopy takes advantage of the selective absorbance of ultraviolet radiation by various substances. The technique is especially useful in investigating biologically active substances such as compounds in body fluids, and drugs and narcotics either in the living body (*in vivo*) or outside it (*in vitro*). Ultraviolet instruments have also been used to monitor air and water pollution, to analyze dyestuffs, to study carcinogens, to identify food additives, to analyze petroleum fractions, and to analyze pesticide residues. Ultraviolet photoelectron spectroscopy, a technique that is analogous to x-ray photoelectron spectroscopy, has been used to study valence electrons in gases.

Microwave spectroscopy, or molecular rotational resonance spectroscopy, addresses the microwave region of the electromagnetic spectrum and the absorption of energy by molecules as they undergo transitions between rotational energy levels. From these spectra, it is possible to obtain information about molecular structure, including bond distances and bond angles. One example of the application of this technique is in the distinction of trans

and gauche rotational isomers. It is also possible to determine dipole moments and molecular collision rates from these spectra.

In nuclear magnetic resonance (NMR), resonant energy is transferred between a radio-frequency alternating magnetic field and a nucleus placed in a field sufficiently strong to decouple the nuclear spin from the influence of atomic electrons. Transitions induced between substrates correspond to different quantized orientations of the nuclear spin relative to the direction of the magnetic field. Nuclear magnetic resonance spectroscopy has two subfields: broadline NMR and high resolution NMR. High resolution NMR has been used in inorganic and organic chemistry to measure subtle electronic effects, to determine structure, to study chemical reactions, and to follow the motion of molecules or groups of atoms within molecules.

Electron paramagnetic resonance is a spectroscopic technique similar to nuclear magnetic resonance except that microwave radiation is employed instead of radio frequencies. Electron paramagnetic resonance has been used extensively to study paramagnetic species present on various solid surfaces. These species may be metal ions, surface defects, or adsorbed molecules or ions with one or more unpaired electrons. This technique also provides a basis for determining the bonding characteristics and orientation of a surface complex. Because the technique can be used with low concentrations of active sites, it has proven valuable in studies of oxidation states.

Atoms or molecules that have been excited to high energy levels can decay to lower levels by emitting radiation. For atoms excited by light energy, the emission is referred to as atomic fluorescence; for atoms excited by higher energies, the emission is called atomic or optical emission. In the case of molecules, the emission is called fluorescence if the transition occurs between states of the same spin, and phosphorescence if the transition takes place between states of different spin.

In x-ray fluorescence, the term refers to the characteristic x-rays emitted as a result of absorption of x-rays of higher frequency. In electron fluorescence, the emission of electromagnetic radiation occurs as a consequence of the absorption of energy from radiation (either electromagnetic or particulate), provided the emission continues only as long as the stimulus producing it is maintained.

The effects governing x-ray photoelectron spectroscopy were first explained by Albert Einstein in 1905, who showed that the energy of an electron ejected in photoemission was equal to the difference between the photon and the binding energy of the electron in the target. In the 1950s, researchers began measuring binding energies of core electrons by x-ray photoemission. The discovery that these binding energies could vary as much as 6 eV, depending on the chemical state of the atom, led to rapid development of x-ray photoelectron spectroscopy, also known as Electron Spectroscopy for Chemical Analysis

(ESCA). This technique has provided valuable information about chemical effects at surfaces. Unlike other spectroscopies in which the absorption, emission, or scattering of radiation is interpreted as a function of energy, photoelectron spectroscopy measures the kinetic energy of the electrons(s) ejected by x-ray radiation.

Mössbauer spectroscopy was invented in the late 1950s by Rudolf Mössbauer, who discovered that when solids emit and absorb gamma rays, the nuclear energy levels can be separated to one part in  $10^{14}$ , which is sufficient to reflect the weak interaction of the nucleus with surrounding electrons. The Mössbauer effect probes the binding, charge distribution and symmetry, and magnetic ordering around an atom in a solid matrix. An example of the Mössbauer effect involves the  $\text{Fe}^{57}$  nuclei (the absorber) in a sample to be studied. From the ground state, the  $\text{Fe}^{57}$  nuclei can be promoted to their first excited state by absorbing a 14.4-keV gamma-ray photon produced by a radioactive parent, in this case  $\text{Co}^{57}$ . The excited  $\text{Fe}^{57}$  nucleus then decays to the ground state via electron or gamma ray emission. Classically, one would expect the  $\text{Fe}^{57}$  nuclei to undergo recoil when emitting or absorbing a gamma-ray photon (somewhat like what a person leaping from a boat to a dock observes when his boat recoils into the lake); but according to quantum mechanics, there is also a reasonable possibility that there will be no recoil (as if the boat were embedded in ice when the leap occurred).

When electromagnetic radiation passes through matter, most of the radiation continues along its original path, but a tiny amount is scattered in other directions. Light that is scattered without a change in energy is called Rayleigh scattering; light that is scattered in transparent solids with a transfer of energy to the solid is called Brillouin scattering. Light scattering accompanied by vibrations in molecules or in the optical region in solids is called Raman scattering.

In vibrational spectroscopy, also known as Raman spectroscopy, the light scattered from a gas, liquid, or solid is accompanied by a shift in wavelength from that of the incident radiation. The effect was discovered by the Indian physicist C. V. Raman in 1928. The Raman effect arises from the inelastic scattering of radiation in the visible region by molecules. Raman spectroscopy is similar to infrared spectroscopy in its ability to provide detailed information about molecular structures. Before the 1940s, Raman spectroscopy was the method of choice in molecular structure determinations, but since that time infrared measurements have largely supplemented it. Infrared absorption requires that a vibration change the dipole moment of a molecule, but Raman spectroscopy is associated with the change in polarizability that accompanies a vibration. As a consequence, Raman spectroscopy provides information about molecular vibrations that is particularly well suited to the structural analysis of covalently bonded molecules, and to a lesser extent, of ionic crystals. Raman spectroscopy is also particularly useful in studying

the structure of polyatomic molecules. By comparing spectra of a large number of compounds, chemists have been able to identify characteristic frequencies of molecular groups, e.g., methyl, carbonyl, and hydroxyl groups.

Spectroscopy has great potential to enhance military and defense capabilities. Both chemical and biological warfare agents are detectable, and potentially identifiable, by spectroscopic imaging. New technology involving fiber optic systems and lasers that can quickly change frequencies provides the opportunity to miniaturize spectroscopic equipment. Systems are currently being developed, which will take this technology into the battlefield in order to target surface and ground contamination by chemical and biological weapons. Spectroscopic examination can also aid in the identification and measurement of subcellular processes, such as carbon dioxide production or oxygen use. These measurements facilitate the understanding of cell growth, cellular response to environmental stimuli, and cellular reactions to drugs and biological and chemical warfare agents.

#### ■ FURTHER READING:

##### PERIODICALS:

Behnisch, P.A. "Biodetectors in Environmental Chemistry: Are We at a Turning Point?" *Environ Int* 27(2001):441-42.

"Early Warning Technology." *Med Device Technol* 13 (2002): 70-72.

Casagrande R. "Technology against Terror." *Scientific American*. 287 (2002):59-65.

##### ELECTRONIC:

Scripps Center for Mass Spectrometry (BC-007), 10550 North Torrey Pines Rd., La Jolla, CA 92037. (858) 784-9596. Gary Suizdak, director. <<http://masspec.scripps.edu/information/intro/index.html>> (January 5, 2003).

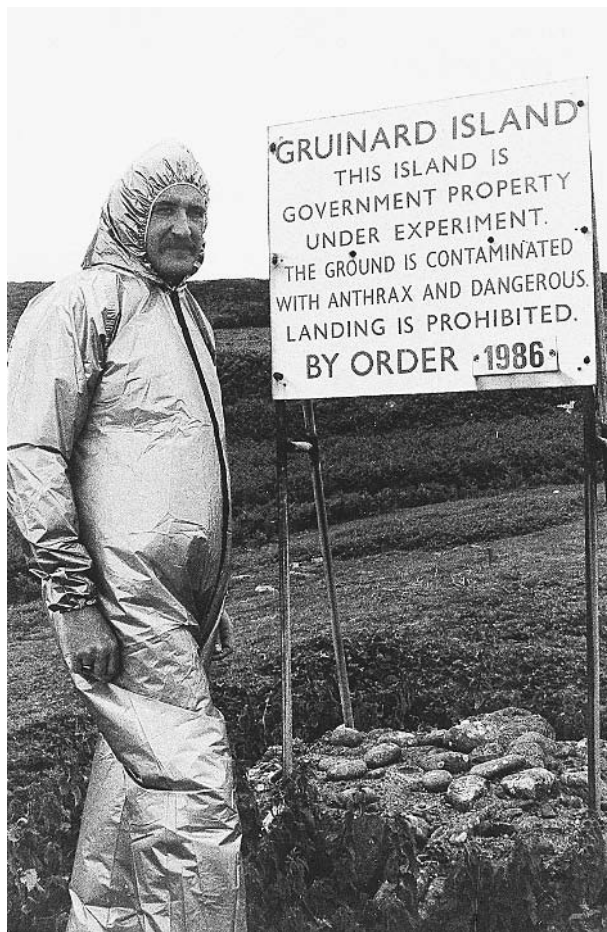
##### SEE ALSO

*Biological Warfare, Advanced Diagnostics*  
*Biomedical Technologies*  
*Chemical and Biological Detection Technologies*  
*Electromagnetic Spectrum*  
*Electromagnetic Weapons, Biochemical Effects*  
*Microscopes*

## Spores

#### ■ BRIAN HOYLE

A spore is a hard casing that contains the genetic material of those bacteria and other microorganisms that are able to form the structure. This physically and chemically resilient package protects the genetic material during periods



A member of the Ministry of Defense Chemical Defense Establishment stands near a warning sign in Gruinard Island, Scotland, the site of explosive munitions testing using anthrax spores as a biological weapon. The island was sealed off from the public for almost 50 years. AP/WIDE WORLD PHOTOS.

when the environmental conditions are so harsh that the growing form of the microbe would be killed.

The effect of temperature on bacterial and spore survival provides a good example of the resilience of bacterial spores. Temperatures of 80 to 90° Celsius (176-194°F) typically kill bacteria that are growing and dividing within minutes. These high temperatures cause structural components of the bacteria to dissolve, and strands of genetic material to separate from one another. A group of bacteria known as thermophilic bacteria can survive these temperatures, but temperatures of 120°C (248°F) kill even thermophiles. In contrast, spores can survive exposure to 120°C for several hours.

Spores of bacteria that subsequently could be revived into the growing form have been recovered from materials that are over a century old. Thus, spores offer an extraordinary form of protection to bacteria. Anthrax spores that could germinate into living bacteria were recovered on Gruinard Island, an island off the coast of Scotland that

was used for biological weapons testing by the British government during World War II.

Spores are noteworthy in terms of security because of the threat they pose in the hands of terrorists. *Bacillus anthracis*, the bacterium that causes anthrax, is a spore former. The spores are very light and tiny. As a result, they can be readily dispersed through the air and can be easily inhaled into the lungs. The resulting lung infection, which is called inhalation anthrax, is almost always fatal without prompt medical treatment. Anthrax spores were used as a mechanism of bioterrorism to target United States citizens by deliberate dispersal in the mail system in late 2001.

Another prominent example of a bacterial spore former of concern is *Clostridium botulinum*. The bacterium and the spore are widespread in nature; for example, they are a common inhabitant of the soil. This bacterium can also survive in canned foods for extended time periods, even when the food has been heated or is acidic. When the food is eaten, the dormant bacteria begin to grow again and produce a variety of potent toxins that disrupt the nervous system, causing serious illness.

The contamination of foods by terrorists is a significant security concern, especially in the United States. Because the spores are hardy and can be transported virtually undetected, they could be taken to food plants or supermarkets, where the food could be contaminated. The spores would survive to cause illness.

Other microorganisms of human concern that form spores include protozoa (e.g., *Microsporidia*) and fungi (e.g., *Actinomyces*).

**Formation of bacterial spores.** The multistep process of forming a spore is known as sporulation. The process begins when a bacterium senses that the environmental conditions are becoming life threatening. Bacteria are equipped with a whole battery of sensing proteins and other compounds that monitor environmental conditions of temperature, pH of the surrounding fluid, water content, and availability of food, as some examples. After monitoring the environment for a period of time, the deteriorating conditions trigger the microbe to begin the change from a growing and dividing cell to a dormant spore.

The genetic material of the bacterium is duplicated. Then, the membrane coat that surrounds the inside of the bacterium pinches inward until the ends of the inward growing membrane meet. This isolates one of the copies of the genetic material from the remainder of the bacterium. This smaller cell is called a daughter cell. The remainder of the bacterium is called the mother cell.

In the next stage of spore formation, the membrane that surrounds the mother cell surrounds the daughter cell. This creates a daughter cell that is surrounded by two layers of membrane. Between these two membranes a thick layer of a rigid material forms. This layer is called peptidoglycan. Peptidoglycan is normally present in the

bacterial cell wall, but not in nearly the same amount. The thick peptidoglycan makes the double membrane layer very tough and hard to break apart. Finally, this tough membrane is coated on the outer surface by proteins. The proteins are also resistant to breakage.

The remnants of the mother cell dissolve away leaving the spore. The spore is essentially in hibernation. There is very little chemical activity. Nevertheless, the spore is able to monitor the external environment and, when conditions are sensed as being more favorable, the conversion from the spore form to the growing organism begins.

**The threat from spores.** The threat from spores, particularly anthrax spores, lies in their small size and powdery texture once they have been dried. As shown in the anthrax attacks in the United States in 2001, anthrax spores can be delivered to someone in a letter. The spores escape detection using methods like an x ray. When the letter is opened, the spores can be dispersed in the air and breathed in.

Studies in animal models have shown that even the inhalation of a few spores is enough to cause an infection. The lung is an ideal environment for the anthrax bacterium. Food is available and the atmosphere is warm and moist. When the spores germinate into growing bacteria, the resulting infection can feel similar to the flu at first. Thus, a victim may not seek treatment, believing that the illness will pass in a few days. By the time the true nature of the infection is discovered, the infection can be so advanced as to be fatal.

Anthrax spores could also potentially be dispersed from an airplane or a balloon. Indeed, the terrorists responsible for the September 11, 2001 attacks on the World Trade Center and the Pentagon had explored the use of crop dusting aircraft. Models developed by the U.S. government have predicted that a few hundred pounds of anthrax spores released upwind of Washington, D.C. could cause at least several hundred thousand deaths within a few days.

The growing of the amounts of bacteria necessary to prepare large amounts of powdered spores and the preparation of the spores is not an easy task. Nonetheless, many microbiologists are capable of the task, and the construction of a facility that is large enough to house the needed equipment is not overly difficult. In the past century, nations including the U.S. and Russia had active anthrax weaponization programs. Prior to Operation Iraqi Freedom, Iraq was suspected of having an anthrax weapons development program.

**Protection from spores.** The threat posed by the use of spores in the mail is difficult to counter. Researchers are working to develop sensors that detect the spores, based on the reaction of antibodies with target proteins on the surface of the spores. However, such detection requires

physical contact with the spores. Methods that do not require the opening of letters, such as irradiation, are being tested and refined in the field and in the laboratory.

Another tact is the use of compounds that can destroy the spore. For example, in 2002, researchers discovered that an enzyme called PlyG lysin will chemically crack apart the spore coat. The spore contents are released and disintegrate. Until such sophisticated detection and protection methods are perfected, the treatment of a site contaminated with spores will continue to include the use of bleach.

## ■ FURTHER READING:

### BOOKS:

Fischetti, Vincent, Richard P. Novick, Joseph J. Ferretti, and Danile A. Portnoy. *Gram-Positive Pathogens*. Washington: American Society for Microbiology Press, 2000.

Storz, Gisela, and Regine Hengge-Aronis. *Bacterial Stress Responses*. Washington: American Society for Microbiology Press, 2000.

Caipo, M.L., S. Duffy, L. Zhao, et al. "Bacillus megaterium Spore Germination is Influenced by Inoculum Size." *Journal of Applied Microbiology*. no. 92 (2002): 879–84.

### ELECTRONIC:

American Society for Microbiology. "Microbial Spore Formation." *Microbe.org*. 1999. <<http://www.microbe.org/microbes/spores.asp>>(10 January 2003).

### SEE ALSO

*Anthrax, Terrorist Use as a Biological Weapon*  
*Anthrax Weaponization*  
*Biological Warfare*  
*Food Supply, Counter-Terrorism*  
*Mail Sanitization*  
*Pathogens*  
*Weapons of Mass Destruction, Detection*

---

## SR-71 Blackbird

---

### ■ CARYN E. NEUMANN

The SR-71, a black, high-altitude airborne reconnaissance platform that flew at transonic speed, gave the United States the ability to photograph military sites in hostile countries as well as the opportunity to confirm interpretations of satellite photographs from 1968 until 1990. Photographs taken from SR-71s helped end the siege of Khe Sanh in Vietnam in 1968, preserved the Strategic Arms Limitation Treaty (SALT) with the Soviet Union by monitoring troop movements in Cuba in 1979, and confirmed that Iran had

acquired Silk Worm missiles from China for possible use against oil tankers in the Straits of Hormuz in 1987. While of obvious military value, each SR-71 burned enormous amounts of fuel, and required a large amount of staff support. For reasons of economy, the Department of Defense terminated the program and the last SR-71 flew in 1990.

The SR-71, planned in the early 1960s as a weapon in the Cold War, gave the U.S. the ability to survey more than 100,000 square miles of Earth's surface in an hour's time. The 29 aircraft in service flew above 80,000 feet, higher than any other platform, and traveled at Mach 3.17–3.30 covering 30 miles every minute. The SR-71 could survey up to a quarter of a million square miles of territory in one sortie. High-strength lightweight titanium alloy covered 90% of the aircraft with 20% of the skin consisting of radar-transparent plastic. For missions, the platforms were fitted with either a high-resolution horizon-to-horizon optical bar camera or a radar package which generated film of the ground in all weather conditions. The SR-71 contained no armament.

The first operational flight of the SR-71 took place on March 21, 1968, and brought information crucial to the American war effort in Vietnam. Photos taken by the crew revealed the location of heavy artillery emplacements around Khe Sanh, an American garrison in Vietnam under siege by the North Vietnamese. By providing data that had previously eluded sensors on other aircraft, the SR-71 allowed the American command to direct B-52 bombers to the enemy site and helped to end an event which had riveted the attention of the public. In 1979, when a satellite revealed a large Soviet force in Cuba, an SR-71 flew continuing surveillance over the island to monitor the situation and ensure Senate ratification of SALT. A 1987 mission to Iran gathered extensive information about masses of military equipment in the Persian Gulf, including the presence of Silk Worms, land-based anti-ship missiles from China that the Iranians apparently intended to use to threaten merchant tankers in the Straits of Hormuz. The U.S. Navy received warning of the missiles and diplomats brought pressure on Iran to remove them. On 80 occasions in the 1980s when satellites broke down or were unable to see through the atmosphere, SR-71s provided reconnaissance imagery of vital areas in the Middle East.

The SR-71 penetrated hostile territory with comparatively little vulnerability to attack unlike other reconnaissance platforms like the U-2 spy plane. The workhorse U-2, however, operated for considerably less money and generally received reconnaissance assignments while the SR-71s remained in their hangars. The Department of Defense made the decision to terminate the program on November 22, 1989. Secretary of Defense Richard Cheney in June 1990 ordered that three SR-71 aircraft be placed into long-term storage for possible use in a future conflict. The SR-71s did not see service in the Gulf War, however, and most of their aircrews and skilled maintenance force





SR-71 Blackbird. ©GEORGE HALL/CORBIS.

are now unavailable because of the passage of time. As satellite technology involves less human risk and grows and more precise and cost-effective, it is uncertain that the United States will justify the cost of deploying SR-71 intelligence-gathering machines in the future.

#### ■ FURTHER READING:

##### BOOKS:

Crickmore, Paul F. *Lockheed SR-71: The Secret Missions Exposed*. London: Osprey, 1988.

Thornborough, Anthony M. *Sky Spies: Three Decades of Airborne Reconnaissance*. London: Arms and Armour Press, 1993.

##### SEE ALSO

*Photographic Resolution  
Photography, High-Altitude  
Satellites, Spy*

## Star Wars.

SEE *Strategic Defense Initiative and National Missile Defense*.

## START I Treaty

■ ADRIENNE WILMOTH LERNER

The Strategic Arms Reduction Treaty, now known as START I, was one of the key weapons agreements forged during the détente period of the late Cold War era. Negotiations for strategic weapon reductions of the United States and Soviet Union arsenals began in 1982, when both nations sought a lessening of Cold War tensions. The initial enthusiasm for the treaty waned when the Soviet Union withdrew from talks regarding weapons reduction after the United States deployed several intermediate-range missiles in allied nations in western Europe. Negotiations did not begin again until 1985, and then progressed slowly until the fall the Iron Curtain and Soviet-influenced communism in Eastern Europe. START I was finally signed by United States President George H. W. Bush and Soviet Premier Mikhail Gorbachev in Moscow on July 31, 1991.

START I called for a drastic reduction of United States and Soviet arsenals. The treaty was originally designed to cover a fifteen-year period, in which the total Cold War build-up of weapons would be reduced to a third of its pre-treaty strength. The two nations agreed to limit strategic

arms, and maintain similarly strengthened arsenals. The treaty covered not only warheads, but also long-range delivery vehicles including Intercontinental Ballistic Missiles (ICBMs). START I limited each nation to 1,600 nuclear delivery vehicles, 6,000 warheads, and less than 7,000 ballistic missile warheads. Both nations began developing plans and facilities for weapons destruction during the negotiation process, however, the United States was better equipped to handle limited disarmament at the time START I was signed.

Though an indication of diminishing Cold War era tensions between the two nations, the treaty was controversial. Some argued that the treaty handicapped new weapons development and downplayed national security threats from other nations aside from the Soviet Union. Environmentalists feared that large-scale weapons destruction would not be adequately planned or contained, causing damage similar to that of already controversial weapons testing.

The largest hurdle to START I, however, came just a few months after its ratification. In 1991, The Soviet Union dissolved, leaving its nuclear arsenal scattered in the newly independent nations of Russia, Ukraine, Kazakhstan, and Belarus. The four Soviet successor states signed an addendum to the START I treaty on May 23, 1992. The Lisbon Protocol to the START I treaty added these nations to the treaty, each agreeing to dismantle their weapons arsenals to meet the provisions of the original treaty. The protocol further bound the nations to a Nuclear Non-proliferation Treaty, strictly curtailing the sale or transmission of nuclear technology to non-nuclear nations and eliminating Soviet-era nuclear weapons from Soviet successor states, with the exception of Russia. Under the Cooperative Threat Reduction (CTR) program, all warheads in Ukraine, Belarus, and Kazakhstan were transferred back to Russia by 1997.

START I does not expire until 2009, but in December 2001, all START I reductions were completed. Russia and the United States signed a subsequent START treaty in 1993, and the Strategic Offensive Reductions Treaty (SORT) in 2002. These treaties further reduce the permitted number of strategic arms, but also address the problems of aging nuclear arsenals and the possibility of long-term weapons storage as an alternative to destruction.

#### ■ FURTHER READING :

##### ELECTRONIC:

United States Department of Energy, *Atomic Century* <[http://www.dpi.anl.gov/dpi2/hist\\_docs/treaties/start2.htm](http://www.dpi.anl.gov/dpi2/hist_docs/treaties/start2.htm)> (20 December 2002).

##### SEE ALSO

START II



An SS-19 strategic missile warhead is loaded into a silo at a site near Saratov, Russia, in 1999. After languishing in the Russian parliament for almost seven years, the START II arms control treaty was finally ratified by Russia in 2000. AP/WIDE WORLD PHOTOS.

## START II

■ ADRIENNE WILMOTH LERNER

START II, or the Further Reduction and Limitation of Strategic Offensive Arms Treaty, was drafted as an expansion of the 1991 Strategic Arms Reduction Treaty (START I). The treaties between Russia and the United States prescribed the reduction of national nuclear warheads, delivery systems, and ballistic missiles. START II proposed to reduce the arsenals of the United States and Russia to a third of their pre-treaty strength.

The second strategic arms reduction treaty was signed in Moscow on January 3, 1993. The treaty was not ratified by the U.S. Senate until three years later. In March 1997, at the Helsinki Summit, an addendum known as the Helsinki Protocol was added to START II and later ratified by both nations. The Helsinki Protocol allowed for an extended amount of time to achieve treaty objectives, giving both nations time to implement new programs for deactivation, storage, and destruction.

START II, with the Helsinki Protocol addendum, called for two phases of reduction. The first phase included a sizable reduction of warheads and demanded the complete deactivation of nuclear warhead delivery systems banned by the treaty by the end of 2004. The second phase proposed a further reduction of warheads and the destruction of deactivated missiles and delivery systems by December 31, 2007.

START II especially addressed post-Cold War relations between Russia and the United States, seeking to reduce the Cold War era build up of arms and forge new Russian-American cooperative strategies in regard to international nuclear policy. The treaty called for both nations to reduce their arsenals to approximately 3,500 warheads. In addition to prescribing further deactivation of warheads, START II expanded limitations on delivery systems such as submarines, bombers, and ballistic missiles. A main American objective of START II negotiations was a ban on all Russian SS-18 missiles. The final treaty banned all current Multiple Independently Targetable Reentry Vehicles (MIRVs) missiles, or heavy ballistic missiles with multiple warheads, in both nations' deployed forces. This provision was mainly targeted at encouraging strategic disarmament in former Soviet satellite nations in Europe and Asia, and the dismantling of Russian and American "first strike capability" weapons.

START II prescribed the same rigid guidelines for weapons counting and destruction as START I. It further utilized the same policing, reporting, and confirmation committees as established by the former treaty.

START II was once again brought into the spotlight in 2002. Earlier moves by the U.S. government to amend, or even dissolve, a separate treaty with Russia regarding ballistic missiles, to allow possible construction of a missile defense system, prompted Russia to reevaluate their interest in continuing with START II arms reductions. In May 2002, U.S. President George W. Bush and Russian President Vladimir Putin signed a new weapons management treaty, the Strategic Offensive Reductions Treaty (SORT).

#### ■ FURTHER READING:

##### ELECTRONIC:

United States Department of Energy, *Atomic Century* <[http://www.dpi.anl.gov/dpi2/hist\\_docs/treaties/start2.htm](http://www.dpi.anl.gov/dpi2/hist_docs/treaties/start2.htm)> (20 December 2002).

---

## STASI

---

The *Ministerium für Staatssicherheit*, Ministry of State Security, was the primary intelligence and security agency

of the German Democratic Republic (GDR), or East Germany, during the Cold War. The Stasi, as the organization was most commonly known, maintained a comprehensive network of informants, agents, and military-trained secret police. Stasi operations focused on political security and espionage, both domestically and abroad, aiding the Soviet KGB more than any other satellite intelligence organization. During its 39-year tenure, at least one-third of the population of East Germany was victimized by Stasi surveillance, arrest, detention, or torture.

The East German government, with the assistance of the Soviet intelligence community, established the Stasi on February 8, 1950. The organization's main charge was preserving the communist regime in East Germany through clandestine operations. The first Stasi agents were trained by the Soviet KGB. From the outset, the Stasi operated above the law. The agency's policies and operations were reviewed only by the Communist Central Committees in East Germany and the Soviet Union; in turn, the agency expressly served the political desires of the communist regime.

The Stasi created a widespread network of civilian informants. These informants were citizens who cooperated with Stasi agents, sometimes in exchange for money or goods. These unofficial informants used their jobs, social influence, and family networks to spy on fellow citizens. Informants were required to report suspicious or anti-government behavior to Stasi authorities. Tips from informants were followed by further agent surveillance or immediate arrest. The Stasi maintained its own network of detention camps and prisons, the most notorious of which was Bauden II. The Stasi garnered a reputation for its use of brutality, torture, and blackmail as routine methods of extracting information and coercing cooperation.

While the threat of Stasi non-member informants was great, the actual agent network of the Stasi was itself comprehensive. The agency used human intelligence to infiltrate factories, schools, and social and political organizations. Stasi officials created vast files on individuals that included photographs, surveillance reports, and even physical samples of hair or clothing. Stasi agents used scent samples, often bits of clothing sealed in airtight containers for storage, to track defectors or known dissidents using dogs.

The Agency itself was divided into several operational divisions, each focusing on various internal security tasks. The Ministry for State Security maintained one armed force, the *Feliks Dzierzynski* Guard Regiment (FD), named for the founder of the Bolshevik secret police. The force consisted of as many as 8,000 military-trained members. The FD guarded government and communist party personnel, government buildings, Soviet monuments, and military installations. The FD employed special commando and intelligence units to conduct clandestine operations.

The Main Administration for Reconnaissance focused its espionage on foreign intelligence, most especially the nations of the North Atlantic Treaty Organizations (NATO)



Workers shown in this 1998 photo reconstituting the Stasi archives which were torn up and put into 17,000 bags. ©BOSSU REGIS/CORBIS SYGMA.

and neighboring West Germany. The division coordinated its intelligence findings with the Soviet KGB via the Main Coordinating Administration.

East Germany was a highly controlled censorship state. The Main Department for Communications Security operated an internal communications network from the East German government and between East German and Soviet authorities. The department also culled government information from public media, and conducted counterespionage measures to secure lines against tapping devices. Surveillance of foreign diplomats, foreign residents, and occasional travelers was conducted by the Main Administration for the Struggle Against Suspicious Persons. Like East German citizens, foreigners in East Germany were subject to strict censorship and Stasi arrest.

Immediately before the fall of East Germany in 1989, the Stasi employed 91,000 staff members. Their active informer network included nearly 200,000 people. After the reunification of Germany on October 3, 1990, the German intelligence community was radically reorganized. In an attempt to restore public trust in the government in the former GDR, German officials banned employment in the new government of anyone who had worked for the East German Stasi. The extensive Stasi archives were opened to the public in 1991, permitting victims of Stasi surveillance to find out the names of agents and informers who had spied on them.

#### ■ FURTHER READING:

##### BOOKS:

Koehler, John O. *STASI: The Untold Story of the East German Secret Police*. Boulder, CO: Westview Press, 1999.

##### SEE ALSO

*Berlin Tunnel*

*Berlin Wall*

*Cold War (1945–1950), The Start of the Atomic Age*

*Cold War (1950–1972)*

*Cold War (1972–1989): The Collapse of the Soviet Union*

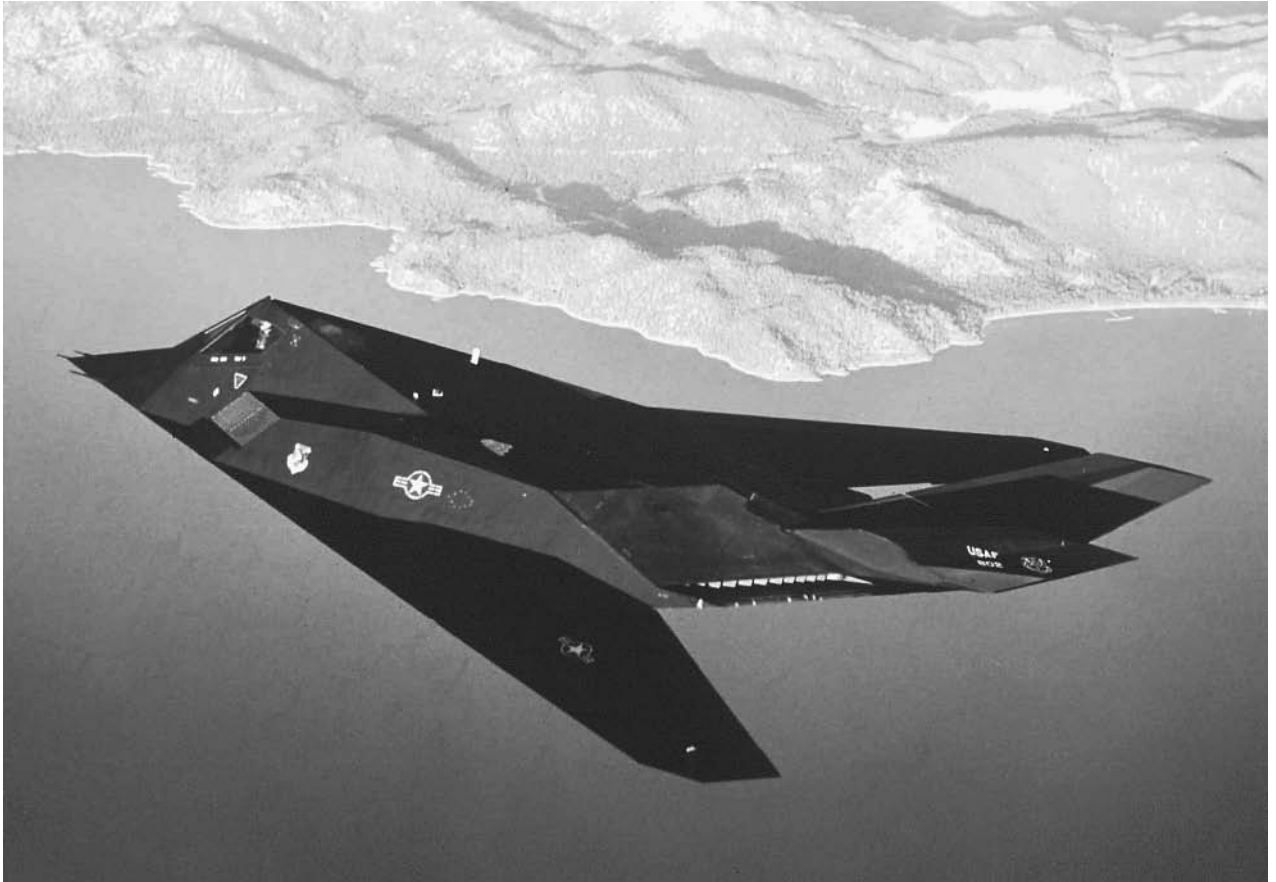
*Germany, Intelligence and Security*

*KGB (Komitet Gosudarstvennoi Bezopasnosti, USSR Committee of State Security)*

## Stealth Technology

#### ■ LARRY GILMAN

Stealth technology, also termed “low-observable” technology, is a set of techniques that render military vehicles, mostly aircraft, hard to observe. Because RADAR—an acronym for *RA*dio *D*etection *A*nd *R*anging—is the



An Air Force F-117 stealth fighter is shown in this undated Department of Defense photo. AP/WIDE WORLD PHOTOS.

primary detection technology for aircraft, most stealth technologies are directed at suppressing RADAR returns from aircraft, but stealth technology minimizes other “observables” as well, including energy emissions that of any kind that might be observed by an opponent. Stealth technology is deployed today on several types of aircraft and a few surface ships. Counter-stealth technologies are also under continuous development.

## History of Stealth Technology

Development of stealth technology for aircraft began before World War I. Because RADAR had not been invented, visibility was the sole concern, and the goal was to create aircraft that were hard to see. In 1912, German designers produced a largely transparent monoplane; its wings and fuselage were covered by a transparent material derived from cellulose, the basis of movie film, rather than the opaque canvas standard in that era. Interior struts and other parts were painted with light colors to further reduce visibility. The plane was effectively invisible from the ground when flown at 900 ft (274 m) or higher, and faintly visible at lower altitudes. Several transparent German aircraft saw combat during World War I, and Soviet aircraft designers attempted the design of transparent aircraft in the 1930s.

With the invention of RADAR during World War II, stealth became both more needful and more feasible: more needful because RADAR was highly effective at detecting aircraft, and would soon be adapted to guiding anti-aircraft missiles and gunnery at them, yet more feasible because to be RADAR-stealthy an aircraft did not need to be completely transparent to radio waves; it could absorb or deflect them.

During World War II, Germany coated the snorkels of its submarines with RADAR-absorbent paint to make them less visible to RADARs carried by Allied anti-submarine aircraft. In 1945 the U.S. developed a RADAR-absorbent paint containing iron. It was capable of making an airplane less RADAR-reflective, but was heavy; several coats of the material, known as MX-410, could make an aircraft unwieldy or even too heavy to fly. However, stealth development continued throughout the postwar years. In the mid 1960s, the U.S. built a high-altitude reconnaissance aircraft, the Lockheed SR-71 Blackbird, that was extremely RADAR-stealthy for its day. The SR-71 included a number of stealth features, including special RADAR-absorbing structures along the edges of wings and tailfins, a cross-sectional design featuring few vertical surfaces that could reflect RADAR directly back toward a transmitter, and a coating termed “iron ball” that could be electronically

manipulated to produce a variable, confusing RADAR reflection. The SR-71, flying at approximately 100,000 feet, was routinely able to penetrate Soviet airspace without being reliably tracked on RADAR.

Development of true stealth aircraft (i.e., those employing every available method to avoid detection by visible, RADAR, infrared, and acoustic means) continued, primarily in the U.S., throughout the 1960s and 1970s, and several stealth prototypes were flown in the early 1970s. Efforts to keep this research secret were successful; not until a press conference was held on August, 22, 1980, after expansion of the stealth program had given rise to numerous rumors and leaks, did the U.S. government officially admit the existence of stealth aircraft. Since then, much information about the two U.S. stealth combat aircraft, the B-2 bomber and the F-117 fighter (both discussed further below), has become publicly available.

Design for stealth requires the integration of many techniques and materials. The types of stealth that a maximally stealthy aircraft (or other vehicle) seeks to achieve can be categorized as visual, infrared, acoustic, and RADAR.

**Visual stealth.** Low visibility is desirable for all military aircraft and is essential for stealth aircraft. It is achieved by coloring the aircraft so that it tends to blend in with its environment. For instance, reconnaissance planes designed to operate at very high altitudes, where the sky is black, are painted black. (Black is also a low visibility color at night, at any altitude.) Conventional daytime fighter aircraft are painted a shade of blue known as "air-superiority blue-gray," to blend in with the sky. Stealth aircraft are flown at night for maximum visual stealth, and so are painted black or dark gray. Chameleon or "smart skin" technology that would enable an aircraft to change its appearance to mimic its background is being researched. Furthermore, glint (bright reflections from cockpit glass or other smooth surfaces) must be minimized for visual stealth; this is accomplished using special coatings.

**Infrared stealth.** Infrared radiation (i.e., electromagnetic waves in the .72–1000 micron range of the spectrum) are emitted by all matter above absolute zero; hot materials, such as engine exhaust gases or wing surfaces heated by friction with the air, emit more infrared radiation than cooler materials. Heat-seeking missiles and other weapons zero in on the infrared glow of hot aircraft parts. Infrared stealth, therefore, requires that aircraft parts and emissions, particularly those associated with engines, be kept as cool as possible. Embedding jet engines inside the fuselage or wings is one basic design step toward infrared stealth. Other measures include extra shielding of hot parts, mixing of cool air with hot exhausts before emission; splitting of the exhaust stream by passing it through parallel baffles so that it mixes with cooler air more quickly; directing of hot exhausts upward, away from ground observers; and the application of special coatings to hot

spots to absorb and diffuse heat over larger areas. Active countermeasures against infrared detection and tracking can be combined with passive stealth measures; these include infrared jamming (i.e., mounting of flickering infrared radiators near engine exhausts to confuse the tracking circuits of heat-seeking missiles) and the launching of infrared decoy flares. Combat helicopters, which travel at low altitudes and at low speeds, are particularly vulnerable to heat-seeking weapons and have been equipped with infrared jamming devices for several decades.

**Acoustic stealth.** Although sound moves too slowly to be an effective locating signal for antiaircraft weapons, for low-altitude flying it is still best to be inaudible to ground observers. Several ultra-quiet, low-altitude reconnaissance aircraft, such as Lockheed's QT-2 and YO-3A, have been developed since the 1960s. Aircraft of this type are ultralight, run on small internal combustion engines quieted by silencer-suppressor mufflers, and are driven by large, often wooden propellers. They make about as much sound as gliders and have very low infrared emissions as well because of their low energy consumption. The U.S. F-117 stealth fighter, which is designed to fly at high speed at very low altitudes, also incorporates acoustic-stealth measures, including sound-absorbent linings inside its engine intake and exhaust cowlings.

**RADAR stealth.** RADAR is the use of reflected electromagnetic waves in the microwave part of the spectrum to detect targets or map landscapes. RADAR first illuminates the target, that is, transmits a radio pulse in its direction. If any of this energy is reflected by the target, some of it may be collected by a receiving antenna. By comparing the delay times for various echoes, information about the geometry of the target can be derived and, if necessary, formed into an image. RADAR stealth or invisibility requires that a craft absorb incident RADAR pulses, actively cancel them by emitting inverse waveforms, deflect them away from receiving antennas, or all of the above. Absorption and deflection, treated below, are the most important prerequisites of RADAR stealth.

**Absorption.** Metallic surfaces reflect RADAR; therefore, stealth aircraft parts must either be coated with RADAR-absorbing materials or made out of them to begin with. The latter is preferable because an aircraft whose parts are intrinsically RADAR-absorbing derives aerodynamic as well as stealth function from them, whereas a RADAR-absorbent coating is, aerodynamically speaking, dead weight. The F-117 stealth aircraft is built mostly out of a RADAR-absorbent material termed Fibaloy, which consists of glass fibers embedded in plastic, and of carbon fibers, which are used mostly for hot spots like leading wing-edges and panels covering the jet engines. Thanks to the use of such materials, the airframe of the F-117 (i.e., the plane minus its electronic gear, weapons, and engines) is only about 10% metal. Both the B-2 stealth

bomber and the F-117 reflect about as much RADAR as a hummingbird

Many RADAR-absorbent plastics, carbon-based materials, ceramics, and blends of these materials have been developed for use on stealth aircraft. Combining such materials with RADAR-absorbing surface geometry enhances stealth. For example, wing surfaces can be built on a metallic substrate that is shaped like a field of pyramids with the spaces between the pyramids filled by a RADAR-absorbent material. RADAR waves striking the surface zig-zag inward between the pyramid walls, which increases absorption by lengthening signal path through the absorbent material. Another example of structural absorption is the placement of metal screens over the intake vents of jet engines. These screens—used, for example, on the F-117 stealth fighter—absorb RADAR waves exactly like the metal screens embedded in the doors of microwave ovens. It is important to prevent RADAR waves from entering jet intakes, which can act as resonant cavities (echo chambers) and so produce bright RADAR reflections.

The inherently high cost of RADAR-absorbent, airframe-worthy materials makes stealth aircraft expensive; each B-2 bomber costs approximately \$2.2 billion, while each F-117 fighter costs approximately \$45 million; the U.S. fields 21 B-2s and 54 F-117s. The Russian Academy of Sciences, however, according to a 1999 report by *Jane's Defense Weekly*, claims to have developed a low-budget RADAR-stealth technique, namely the cloaking of aircraft in ionized gas (plasma). Plasma absorbs radio waves, so it is theoretically possible to diminish the RADAR reflectivity of an otherwise non-stealthy aircraft by a factor of 100 or more by generating plasma at the nose and leading edges of an aircraft and allowing it flow backward over the fuselage and wings. The Russian system is supposedly lightweight (>220 lb [100 kg]) and retrofittable to existing aircraft, making it the stealth capability available at least cost to virtually any air force. A disadvantage of the plasma technique is that it would probably make the aircraft glow in the visible part of the spectrum.

**Deflection.** Most RADARs are monostatic, that is, for reception they use either the same antenna as for sending or a separate receiving antenna colocated with the sending antenna; deflection therefore means reflecting RADAR pulses in any direction other than the one they came from. This in turn requires that stealth aircraft lack flat, vertical surfaces that could act as simple RADAR mirrors. RADAR can also be strongly reflected wherever three planar surfaces meet at a corner. Planes such as the B-52 bomber, which have many flat, vertical surfaces and RADAR-reflecting corners, are notorious for their RADAR-reflecting abilities; stealth aircraft, in contrast, tend to be highly angled and streamlined, presenting no flat surfaces at all to an observer that is not directly above or below them. The B-2 bomber, for example, is shaped like a boomerang.

A design dilemma for stealth aircraft is that they need not only to be invisible to RADAR but to *use* RADAR;

inertial guidance, the Global Positioning System, and laser RADAR can all help aircraft navigate stealthily, but an aircraft needs conventional RADAR to track incoming missiles and hostile aircraft. Yet the transmission of RADAR pulses by a stealth aircraft wishing to avoid RADAR detection is self-contradictory. Furthermore, RADAR and radio antennas are inherently RADAR-reflecting.

At least two design solutions to this dilemma are available. One is to have moveable RADAR-absorbent covers over RADAR antennas that slip aside only when the RADAR must be used. The antenna is then vulnerable to detection only intermittently. Even short-term RADAR exposure is, however, dangerous; the only stealth aircraft known to have been shot down in combat, an F-117 lost over Kosovo in 1999, is thought to have been tracked by RADAR during a brief interval while its bomb-bay doors were open. The disadvantage of sliding mechanical covers is that they may stick or otherwise malfunction, and must remain open for periods of time that are long by electronic standards. A better solution, presently being developed, is the plasma stealth antenna. A plasma stealth antenna is composed of parallel tubes made of glass, plastic, or ceramic that are filled with gas, much like fluorescent light bulbs. When each tube is energized, the gas in it becomes ionized, and can conduct current just like a metal wire. A number of such energized tubes in a flat, parallel array, wired for individual control (a "phased array"), can be used to send and receive RADAR signals across a wide range of angles without being physically rotated. When the tubes are not energized, they are transparent to RADAR, which can be absorbed by an appropriate backing. One advantage of such an array is that it can turn on and off very rapidly, and only act as a RADAR reflector during the electronically brief intervals when it is energized.

## Stealthy Flying

Stealth technology is most effective when combined with other measures for avoiding detection. For example, the F-117 and B-2 are both designed to fly at night, the most obvious visual stealth measure. Further, the F-117 is designed to fly close to the ground (i.e., at less than 500 feet [152 m]). Normal ground-based RADAR cannot see oncoming targets until they are in a line of direct sight, which, for a fast, low-flying aircraft approaching through hilly terrain, may not occur until the aircraft is almost above the RADAR. Even down-looking RADARs carried on aircraft have more difficulty tracking craft that are flying near ground-level, mingling their reflections with the noisy pattern of echoes from the ground itself ("ground clutter"). The F-117 therefore can fly close to the ground, swerving under computer control to avoid obstacles such as hills or towers. This flight style is known as jinking, snaking, or terrain following. (An aircraft such as the B-2 is too large to perform the rapid maneuvers required for jinking, and so flies at higher altitudes.)

At the opposite extreme from jinking flight, ultra-high altitudes have also been used for stealth purposes. Reconnaissance aircraft deployed by the U.S. since the 1950s, including the U-2 and the SR-71, have set most of the altitude records for “air-breathing” craft (i.e., craft that do not, like rockets, carry their own oxygen). Such planes fly near the absolute limit of aerodynamic action; if they went any higher, there would be not be enough air to provide lift.

**Counter-stealth.** An aircraft cannot be made truly invisible. For example, no matter how cool the exhaust vents of an aircraft are kept, the same amount of heat is always liberated by burning a given amount of fuel, and this heat must be left behind the aircraft as a trail of warm air. Infrared-detecting devices might be devised that could image this heat trail as it formed, tracking a stealth aircraft.

Furthermore, every jet aircraft leaves swirls of air—vortices—in its wake. Doppler RADAR, which can image wind velocities, might pinpoint such disturbances if it could be made sufficiently high-resolution.

Other anti-stealth techniques could include the detection of aircraft-caused disturbances in the Earth’s magnetic field (magnetic anomaly detection), networks of low-frequency radio links to detect stealth aircraft by interruptions in transmission, the use of specially shaped RADAR pulses that resist absorption, and netted RADAR. Netted RADAR is the use of more than one receiver, and possibly more than one transmitter, in a network. Since stealth aircraft rely partly on deflecting RADAR pulses, receivers located off the line of pulse transmission might be able to detect deflected echoes. By illuminating a target area using multiple transmitters and linking multiple receivers into a coordinated network, it should be possible to greatly increase one’s chances of detecting a stealthy target. No single receiver may record a strong or steady echo from any single transmitter, but the network as a whole might collect enough information to track a stealth target.

**Stealth in wartime.** Stealthy jet aircraft have been used for surveillance since the 1950s, but dedicated-design stealth warplanes were not used in combat prior to the first Gulf War (1991). In that war, F-117s—which first became operational in 1982—made some 1,300 sorties and were the only aircraft to bomb targets in downtown Baghdad. B-2 bombers were first used in combat in the Kosovo conflict in 1999, flying bombing sorties from Missouri to Yugoslavia (with midflight refueling over the Atlantic). F-117s were also used in the Kosovo conflict; one was shot down and two were damaged by enemy fire. The first overseas combat deployment of B-2 bombers occurred in 2003, during Operation Iraqi Freedom.

Stealth technology is also employed in U.S. cruise missiles such as the Tomahawk and the AGM-129A. The Tomahawk, a tactical weapon that can carry either nuclear

or conventional warheads, has been deployed in four versions, including air-, sea-, and ground-launched types, and was used extensively in combat in both Gulf Wars and in Afghanistan in 2002. The AGM-129A is stealthier than the 1970s-vintage Tomahawk; it carries the W80 250-kiloton nuclear warhead and is designed to be fired from under the wings of the B-52H Stratofortress strategic bomber. The AGM-129A has not been used in combat.

#### ■ FURTHER READING:

##### BOOKS:

Jones, Joseph. *Stealth Technology*. Blue Ridge Summit, PA: TAB Books, 1994.

##### PERIODICALS:

Hume, Andrew L., and Christopher Baker. “Netted RADAR Sensing,” in *Proceedings of the CIE International Conference on RADAR, (IEEE)* 110–14, 2001.

##### ELECTRONIC:

“Russians Offer Radical Stealth Device for Export.” *Jane’s Defence Weekly*. March 17, 1999. <<http://www.aeronautics.ru/plasma04.htm>> (March 20, 2003).

##### SEE ALSO

*SR-71 Blackbird*  
*U-2 Incident*  
*U-2 Spy Plane*

---

## Steganography

---

#### ■ LARRY GILMAN

Steganography (from the Greek for “covered writing”) is the secret transmission of a message. It is distinct from encryption, because the goal of encryption is to make a message difficult to read while the goal of steganography is to make a message altogether invisible. A steganographic message may also be an encrypted as an extra barrier to interception, but need not be. Steganography has the advantage that even a talented code-cracker cannot decipher a message without knowing it is there.

Steganography has been used since ancient times; Greek historian Herodotus records how one plotter of a revolt communicated secretly with another by shaving a slave’s head, writing on his scalp, letting his hair grow back, and sending the slave as an apparently unencumbered messenger. The number of ways in which a steganographic message might be sent is limited only by human ingenuity. A photograph of a large group of people, for example, might contain a Morse-code message in the expressions



of the people in the photograph (e.g., smiling for dot, blank for dash) or in the directions they are looking (e.g., slightly to the left for dot, straight at the camera for dash). Writing in invisible ink or miniaturizing a message, as on microfilm, are also forms of steganography. Probably the commonest form of steganography involves the embedding of messages in apparently innocent texts, with the letters or words of the message indicated either by subtle graphic emphasis (e.g., heavier ink, lighter ink, a small defect) or by special positioning. For instance, reading the first word of every sentence in what appears to be an ordinary letter might yield a steganographic message.

Like most other forms of cryptography and secret writing, steganography has thrived in the digital era. Most digital documents contain useless or insignificant areas of data, or involve enough redundancy that some of their information can be altered without obvious effect. For instance, one might conceal a message bitstream inside a digital audio file by replacing the least-significant bit of every waveform sample (or every  $n^{\text{th}}$  waveform sample) with a message bit; the only effect on the file, if played back as audio, would be a slight decrease in the sound quality (probably imperceptible). Although steganographic messages can be hidden in any kind of digital files, image files, because they contain so much data to begin with, are usually used for digital steganography. Today a number of commercial or shareware programs exist for encoding text into steganographic images (“stego-images”), and are used by millions of people worldwide who wish to evade surveillance, especially by governments. This includes people who have reason to fear punishment for expressing their political ideas, as well as terrorists.

After the terrorist attacks of September 11, 2001, U.S. officials claimed that members of the group al-Qaeda, as well as of other terrorist groups, had used steganographic software to communicate plans to each other, hiding messages in images on pornographic Web sites and in sports chat rooms. Training camps for extremists in a number of countries now include instruction in cryptographic techniques, including digital steganography.

Steganography is also used for the less dramatic purpose of *watermarking*, which is the hiding of information indicating ownership or origin inside a digital file. (Physical watermarking, the practice after which digital watermarking is named, is the impression of a subtle pattern on paper using water. A watermark is only visible when the paper is held up to a light.) Watermarking can be used for digital authentication (i.e., to prove that certain party was indeed the source of a file) or to check whether a digital file was obtained in violation of copyright.

#### ■ FURTHER READING:

##### BOOKS:

Kippenhahn, Rudolf. *Code Breaking: A History and Exploration*. Woodstock, NY: Overlook Press, 1999.

##### ELECTRONIC:

Johnson, Neil. “Steganography: Seeing the Unseen.” IEEE Computer, February 7, 2001, 26–34. <<http://www.jjtc.com/pub/r2026.pdf>> (April 2, 2003).

Kelley, Jack. “Terror Groups Hide Behind Web Encryption.” USA Today. February 5, 2001. <<http://www.usatoday.com/tech/news/2001-02-05-binladen.htm>> (April 2, 2003).

McCullagh, Declan. “Bin Laden: Steganography Master?” Wired News. February 7, 2001. <<http://www.wired.com/news/politics/0,1283,41658,00.html>> (April 2, 2003).

##### SEE ALSO

*Cryptology, History*

---

## Strategic Defense Initiative and National Missile Defense

---

■ LARRY GILMAN

Since the advent of ballistic missiles at the end of World War II, the United States has considered several anti-ballistic missile (ABM) systems designed to defend against attack by intercontinental ballistic missiles (ICBMs) or, more recently, by shorter-range ballistic missiles. The Strategic Defense Initiative program and its successor, National Missile Defense (NMD), are the two most ambitious ABM schemes proposed to date. SDI sought, according to President Ronald Reagan’s original vision (1983), a space-based ballistic-missile defense system that would render the United States safe from even an all-out Soviet attack involving thousands of missiles; NMD, evolved from SDI concepts in the post-Soviet environment, seeks effectiveness against launches of only one or a few missiles, possibly from “rogue states” such as North Korea. NMD thus returns to the limited design goals of the United States earliest ballistic-missile defense concepts of the 1960s.

Research on ABM systems began in the early 1950s. By the late 1960s, a nuclear-tipped interceptor missile dubbed Sentinel had been developed. Sentinel was designed to destroy incoming warheads by detonating near them, and was intended for deployment around major cities to protect them against accidental launch of one or several Soviet missiles or against a limited strike by China. The system was never deployed, however, and in 1969 President Richard Nixon announced that Sentinel would be renamed Safeguard and reassigned to protecting “our land-based retaliatory forces [i.e., nuclear-tipped ICBMs based in the American Midwest] against a direct attack by the Soviet Union.” At this time, however, the United States and Soviet Union were nearing agreement that ballistic-missile defense (BMD) is inherently destabilizing.



U.S. President Ronald Reagan is flanked by physicist Dr. Edward Teller, left, and Lt. Gen. James A. Abrahamson, director of Strategic Defense Initiative, as he arrives to address a conference marking the first five years of his “Star Wars” missile defense program in 1988. AP/WIDE WORLD PHOTOS.

According to the standard anti-BMD argument, missile defenses encourage their possessor to start a nuclear war strategy because any BMD system will necessarily be more effective against a weakened counterattack than against a first strike; BMD therefore makes it “rational” to attack first. BMD proponents responded that missile defenses would enhance stability by adding to the uncertainties of a first strike. Nobody, during this period, argued that a perfect shield against nuclear attack was technically possible.

The Anti-Ballistic Missile Treaty of 1972 made the anti-BMD point of view official by forbidding the Soviet Union or United States to deploy extensive missile defenses. Each superpower was allowed by the original treaty to build ABM installations at two “widely separated” locations, each with at most 100 interceptor missiles. In 1974, a protocol was added to the ABM Treaty that reduced the number of permitted installations to one per nation. The United States chose to build its permitted ABM system near an ICBM base in Grand Forks, North

Dakota; the Soviet Union deployed a system around Moscow. The Soviet system remains operational to this day, but the United States ABM system was shut down after only 9 months of operation in 1974–75 due to high operating costs and because strategists felt that the system was too small to make any strategic difference.

The ABM treaty’s ban on significant defenses left deterrence through “mutually assured destruction” as an undisputed fact of life; that is, strategists hoped that neither superpower would dare start a nuclear war because annihilation of both societies would be the certain result. On March 23, 1983, however, President Reagan made a televised speech in which he declared that this situation was unacceptable. He asked, “Wouldn’t it be better to save lives than to avenge them? . . . What if free people could live secure in the knowledge that their security did not rest upon the threat of instant U.S. retaliation to deter a Soviet attack, that we could intercept and destroy strategic ballistic missiles before they reached our soil or that of our allies?” This policy—far more ambitious than any ABM concept that had been contemplated before—was formalized by Reagan in National Security Decision Directive 85 two days later. Studies of the feasibility of an SDI-type system were made in the coming months, and a Strategic Defense Initiative Organization (SDIO) was chartered by Secretary of Defense Caspar Weinberger in April 1984.

Reagan’s original proposal was conceptual, not technically specific. In October 1985, the SDIO released a set of five “architecture” studies describing possible configurations for an SDI system. The favored architecture suggested seven defensive layers, including air-, land-, sea-, and space-based components to track and shoot down ballistic missiles during their boost, cruise, and descent phases of flight. The main emphasis was on space-based defenses. Hundreds of satellites were proposed for command, control, and communications; remote sensing; battle management; and actual shutdown of targets.

A few of SDI’s many proposals for destroying enemy missiles during each phase of flight, along with some of the countermeasures proposed for each proposal, are described below. Countermeasures are emphasized because many scientists and engineers in government, academia, and industry argued in the 1980s that it would be relatively easy to defeat SDI’s proposed defenses using countermeasures, so no SDI system could ever replace deterrence. Today’s debate concerning the feasibility of a more limited NMD program revives many of the measure-countermeasure concepts that were discussed during the SDI debate.

## Proposals for Boost-Phase Intercept

The SDIO and its critics were agreed that it would be essential to destroy many enemy missiles during boost phase, the period during which a ballistic missile is being

accelerated by its rocket engines. With existing missile technology, boost phase lasts for 3 to 5 minutes. Boost-phase intercept is essential to defense against a large-scale ballistic missile attack because once the payload of a missile is no longer being accelerated, it can detach from its booster rocket and begin releasing independently targeted warheads (as many as 10 per missile) and hundreds of decoys (i.e., objects designed to confuse sensors). Once a large number of ballistic weapons achieve cruise phase, a “threat cloud” of hundreds of thousands of objects, mostly decoys, could be encountered. It would be impractical, for any defensive system of plausible size, to target every object in such a threat cloud during the few minutes available for cruise-phase defense; therefore, the size of the threat cloud has to be reduced by destroying missiles during boost phase. Some of the methods proposed for boost-phase intercept, along with countermeasures proposed for them, are discussed below.

**Space-based directed-energy weapons.** For boost-phase intercept the SDIO proposed several hundred satellites armed with powerful (i.e., >100 MW) lasers. Microwaves and neutral-particle beams (beams of hydrogen atoms) were also considered, but lasers were, and remain, the more developed technology. The directed-energy concept was, in essence, simple: lasers would cook boosters. Boosters contain flammable fuel and sensitive electronics and cannot carry armor because it would weigh too much, and so are more vulnerable to laser damage than, say, separated warheads, which are armored against the high heat of atmospheric reentry. Directed-energy weapons have two advantages for boost-phase intercept: First, they reach their targets in effectively zero time (at the speed of light or, in the case of a particle beam, at about half the speed of light). Second, after destroying one booster a directed-energy weapon can be retargeted, so each weapon can destroy a number of boosters. A basic limitation of any directed-energy weapon, however, is that it must illuminate or “dwell” on a booster for some period of time to destroy it. Dwell time for a laser of realistic power is generally estimated at between 1 second and 1 minute. Furthermore, redirection of the beam takes time, as it requires swiveling a mirror or other device. Finite dwell times and retargeting times, combined with the short duration of boost phase, place limits on the number of boosters that each directed-energy weapon can, in theory, destroy.

Space-based directed-energy weapons have the further limitation that beam intensity diminishes approximately with the square of the distance. They would therefore have to be placed in low (i.e., 120–3100 mi [200–5,000 km]) polar orbits, waiting to destroy boosting missiles not far below them. Low orbits, however, produce “absenteeism.” That is, a low-orbit satellite can only see a small portion of the Earth at any one time, and so is absent from the sky over a particular area (e.g., Siberia) most of the time. To provide continuous coverage of a given area

therefore requires many satellites. Absenteeism multiplies the number of weapon satellites needed to cover a specific launch zone by a factor of between 6 and 20; that is, for every satellite that happens to be passing over, say, Siberia at a given moment, at least six (or as many as 20) would have to be orbiting elsewhere, waiting their turn.

**Surface-based directed-energy weapons.** Two other SDIO proposals for boost-phase intercept using directed-energy weapons were made. First was the use of fixed, ground-based optical lasers stationed in the continental United States. These lasers would send their beams up to orbital “fighting mirrors” which would reflect their energy back down over the horizon to enemy ballistic missiles in boost phase. The fighting mirrors would swivel rapidly to aim the laser light at the boosters. The lack of maneuverable mirrors that could reflect so much power without being destroyed by it was a major obstacle to this concept. Another technology, intensively urged by the SDIO for several years, was the nuclear-pumped x-ray laser. By surrounding a nuclear bomb with appropriate materials, it is possible in theory to cause those materials to lase (emit laser radiation, in this case in the x-ray part of the spectrum) briefly when the bomb explodes. If even a small fraction of the bomb’s explosive energy is converted into x-ray laser energy, and this energy can be precisely aimed and focused, pulses powerful enough to destroy distant missiles could be generated. A basic limitation on this concept is that x rays cannot travel very far through the atmosphere; like space-based directed energy weapons (with the possible exception of optical-frequency lasers), nuclear-pumped x-ray lasers can only attack boosters during the portion of the boost phase that is above the densest part of the atmosphere, that is, above 50 to 56 miles (80–90 km). It was therefore proposed that nuclear-pumped x-ray lasers be deployed in a “pop-up” system. That is, they would be mounted on missiles deployed on land or at sea not far from the Soviet Union (or other potential enemy). When orbiting detectors observed the infrared signatures of ballistic missile launches (i.e., the infrared glow of hot rocket exhausts), the missiles bearing the nuclear-pumped x-ray laser devices would be launched within a few seconds (i.e., would “pop up”). They would race to the edge of space and there explode, destroying their targets before they could finish boost phase.

## Proposals for Boost-Phase Countermeasures

**Fast-burn boosters.** As described above, boost-phase intercept must by definition gain access to target missiles during their boost phase, which lasts only 3 to 5 minutes. What is more, pop-up x-ray lasers and most proposed space-based directed-energy weapons can reach their targets only during that fraction of the boost phase which takes place in near-vacuum, because lasers and particle

beams tend to be scattered and absorbed by the atmosphere. Therefore, an important boost-phase countermeasure would be to build boosters that accelerate rapidly (“fast burn” boosters). With fast-burn boosters, boost phase would take place entirely within the atmosphere, reducing or eliminating the defense’s chances for boost-phase interception using space-based or pop-up directed-energy weapons. Fast-burn boosters would in any case give boost-phase intercept less time to operate, which would require the defense to build more satellites, which could eventually become prohibitively expensive.

*Booster hardening.* Boosters could be coated with a material that ablates, or vaporizes, when illuminated by laser light. Such a coating could increase the dwell time needed to destroy a booster, again forcing the defense to build more satellites in order to cope with a given number of boosters in the time available.

*Rotation.* Boosters could be designed to spin as they fly. This would spread energy from an attacking laser over a larger surface area, increasing dwell time.

*Decoys.* Cheap rockets that simulate the infrared signature of real, weapons-carrying boosters could be deployed alongside real boosters. Such decoys could be made so numerous that no affordable defensive system could attack them all. Although decoy rockets might stagger and veer after launch, unlike real boosters, the real boosters might be deliberately programmed to stagger and veer like the cheap imitations, further confounding the defense. The later technique is termed “antisimulation”: making a real weapon behave like a cheap decoy, rather than trying to make a cheap decoy that behaves like a real weapon.

*Space mines.* All space-based components of any SDI or NMD system would be vulnerable to space mines, which are simply bombs (possibly nuclear) orbiting near the defensive system’s satellites. Before launching its ICBMs, the attacker would detonate its space mines. Since only one space mine is needed per battle station, and bombs are simpler than megawatt lasers, space mining would be intrinsically cheaper than defense building.

*Kinetic weapons.* Kinetic weapons (also termed “kinetic-kill weapons”) destroy by virtue of their kinetic energy, that is, by colliding with their targets at high speed. Clouds of pellets orbited in the opposite direction to defensive satellites—released, probably, by space mines in appropriate orbits—could strike their targets at tens of thousands of miles per hour.

*Directed-energy weapons.* All the devices proposed for boost-phase intercept, including nuclear-pumped x-ray lasers, would be effective antisatellite weapons, and could therefore be used against an opponent’s defensive satellites even more readily than they could be used against an opponent’s missiles.

*Nonballistic weapons.* An enemy might employ weapons that do not have a boost phase at all. Cruise missiles (which fly at very low altitudes and can be made stealthy to both radar and infrared tracking), crewed aircraft, and

bombs smuggled aboard ships or across land borders are all possible methods of making a nuclear attack that would not be vulnerable to boost-phase intercept.

## Proposals for Cruise-Phase Intercept

SDI envisioned using the same orbital directed-energy stations described above for both boost-phase intercept and for cruise-phase intercept. However, SDI’s designers anticipated that during cruise phase the task of distinguishing between actual warheads and the hundreds of thousands of radar reflectors, decoys, and other objects released after boost phase would become paramount. There would simply be too many objects to attack if one could not tell the warheads from the chaff and decoys. It was therefore proposed that “tapping” each object with a laser pulse and measuring its change in velocity might be used to determine which objects were heavy enough to be warheads; directed-energy weapons would then be used to destroy the real warheads.

## Countermeasures for Cruise Phase

The primary cruise-phase countermeasure would be the release of large numbers of decoys. Atmospheric nuclear explosions could also be used to confuse or blind infrared sensors by providing a glowing background (as seen from space), and all methods mentioned above for destroying defensive satellites—orbital or ground-based directed-energy weapons, space mines, kinetic weapons, and so on—would also be threats to cruise-phase defense. Reactive decoy balloons that sensed a laser tap and accelerated themselves to mimic the mass of a real warhead were proposed as a countermeasure to “weighing” using laser pulses.

## Proposals for Descent-Phase Intercept

Descent phase (also known as “terminal phase”) is the period during which a warhead is falling through the atmosphere toward its target. Descent-phase intercept has the advantage that atmospheric friction will strip away all decoys released during cruise phase, sifting out the real warheads. Descent-phase intercept was the traditional, pre-SDI focus of ballistic-missile defense; the Sentinel system, for example, was designed to use high-altitude nuclear explosions to knock out enemy warheads in descent phase, and the primary focus of post-SDI ballistic-missile defense concepts has also been on descent-phase intercept. Since electromagnetic pulse (EMP) from high-altitude nuclear explosions could cripple communications and electrical systems over a continent-sized area, descent-phase intercept concepts since Sentinel have focused on kinetic-kill weapons that would actually strike their targets.

## Countermeasures for Descent Phase

Possible countermeasures for descent phase are few, but stealth technology could make warheads harder to track; furthermore, the attacker is favored in descent phase by the great speed and small size (>1.5 m long, >.5 m wide at the base) of each cone-shaped warhead. To strike even a single incoming warhead moving at some 10,000 miles per hour, much less hundreds or thousands of them simultaneously, is an extremely difficult rocketry problem, often compared to hitting a bullet with a bullet in midair. Since the inception of the SDI program a number of tests have been conducted in which kinetic weapons (also termed “kinetic kill vehicles”) have intercepted, or sought to intercept, incoming missiles or warhead-like objects, but most tests have failed or produced ambiguous results. Nevertheless, kinetic descent-phase intercept is not impossible, and continuing technological advances may render it more reliable.

The measures-countermeasures debate was vigorous during the 1980s because both sides agreed that a defensive system that allowed even 1% of the Soviet Union’s 8,000 or so strategic warheads to reach the United States—80 thermonuclear weapons—could not protect United States society from destruction. The technical side of the SDI debate therefore revolved around the question of whether a BMD system providing better than 99% defensive coverage was buildable or not, and if so, whether it could be built within a plausible budget. In general, the countermeasures school prevailed. SDI funding was cut back in the late 1980s and the SDIO retreated from its original goal of “render[ing] nuclear weapons impotent and obsolete” (in President Reagan’s 1983 words) to the traditional concept of defense against *limited* ballistic-missile attack. The SDIO was renamed the Ballistic-Missile Defense Organization (BMDO) in May, 1993, and its official emphasis was shifted away from space-based defenses, marking the end of the SDI period.

### After SDI: GPALS and NMD

Three years before the term “strategic defense initiative” was abandoned, SDI officially gave up on being the total nuclear umbrella proposed by President Reagan in 1983. At the order of President George H. Bush, the program assumed in 1990 a more limited mission: Global Protection against Limited Strikes (GPALS). GPALS resembled Sentinel, in seeking to defend only against accidental or small-scale ballistic attacks, rather than massive launches of thousands of missiles. It differed from pre-SDI ballistic-missile defense in that it envisioned *global* protection, especially “theatre” defense against ballistic missiles fired in extended combat zones far from the continental United States.

During the 1990s, the term National Missile Defense (NMD) replaced GPALS, and the program re-evolved many

features of SDI, albeit on a smaller scale. Today, NMD proposes a system with boost-phase, cruise-phase, and descent-phase intercept layers, much like SDI, only not intended to cope with the simultaneous launch of thousands of attacking missiles.

For boost-phase intercept NMD proposes lasers, both airborne and space-based. The airborne laser—already built and test-flown, and scheduled to attempt its first missile shoot-down test in 2003 or 2004—would be flown on a modified Boeing 747, use hydrogen fluoride lasing in the infrared part of the spectrum, have a range of several hundred kilometers, and be directed against theatre (short- and medium-range) ballistic missiles. Adaptive optics that measure atmospheric distortion between the weapon and the target would be an essential component of such a system. Having measured the atmospheric distortion in real time, the weapon imparts an inverse distortion to the laser beam as it fires; the predistortion and the actual atmospheric distortion cancel each other out, allowing a focused beam to dwell on the missile. (A similar technique is widely applied in ground-based astronomy.) NMD also proposes to eventually use space-based lasers for boost-phase intercept. The weapons proposed, a product of research begun under SDI, would consist of infrared (hydrogen fluoride) lasers in low orbits. However, the technical hurdles to such a system are numerous, even disregarding possible countermeasures, and funding for the space-based boost-intercept component of NMD has lately been reduced.

For both cruise and descent (midcourse and terminal) defense, NMD proposes to use kinetic-kill warheads that would destroy by collision. Both land-based and sea-launched kinetic-kill missiles are under development for these phases of defense.

**NMD architecture.** The detailed structure of the proposed NMD shift frequently, depending on technological and political factors. One typical, recently proposed NMD architecture consists of six essential elements:

1) A satellite system for the detection and tracking of missile launches, the first components to be launched in 2006 or 2007. The system consist of six geosynchronous satellites designed to observe the infrared emissions of booster rockets.

2) Approximately five ground-based early-warning radars to project the approximate trajectories of missiles detected by the infrared satellite system.

3) A number of high-frequency ground-based radars in the United States, United Kingdom, Greenland (Denmark), South Korea, and perhaps other locations, designed to discriminate between warheads and decoys during the cruise phase.

3) A midcourse (exoatmospheric) kinetic-kill interceptor missile, to be guided by information received from ground radars. The kinetic-kill warhead or vehicle is thrown

by its booster as nearly as possible toward its target, then guides itself during final approach using onboard sensors, computers, and steering rockets.

4) A "Battle Management, Command, Control, and Communications" network of ground stations where computers will integrate information from sensors, fire and guide interceptors, and assess success and failure in real time so that multiple attempts can be made on a given target if necessary.

The United States withdrew from the ABM Treaty in 2002, allowing it to begin construction on a preliminary cruise-phase kinetic-kill interceptor site in June 2002, in Fort Greely, Alaska. The 16-missile complex is scheduled for completion in 2004.

## ■ FURTHER READING:

### BOOKS:

Causewell, Erin V. *National Missile Defense: Issues and Developments*. New York: Novinka Books, 2002.

Drell, Sidney D., Philip J. Farley, and David Holloway. *The Reagan Strategic Defense Initiative: A Technical, Political, and Arms Control Assessment*. Cambridge, MA: Ballinger Publishing Co., 1990.

### PERIODICALS:

Bethe, Hans A., et al. "Space-Based Ballistic-Missile Defense." *Scientific American*. (October, 1984).

Fowler, Charles. "National Missile Defense (NMD)." *IEEE Aerospace and Electronic Systems Society (AESS) Systems Magazine* (January, 2002):4–12.

Lewis, George N., and Theodore A. Postol. "Future Challenges to Ballistic-Missile Defense." *IEEE Spectrum* (September, 1997): 6–68.

### SEE ALSO

*Ballistic Missiles*  
*Cold War (1945–1950), The Start of the Atomic Age*  
*Cold War (1950–1972)*  
*Cold War (1972–1989): The Collapse of the Soviet Union*

## Strategic Petroleum Reserve, United States

■ WILLIAM J. ENGLE

The Strategic Petroleum Reserve (SPR), located in the United States and operated by the Department of Energy (DOE), is the largest emergency supply system of oil in the world. To enhance national security, in a Presidential Order signed November 13, 2001, President George W.

Bush ordered the U.S. Department of Energy (DOE) to fill the Strategic Petroleum Reserve. The oil will come from royalty-in-kind transfers between the Department of the Interior and the DOE.

The SPR is designed to act as a "first line of defense" against a reduction of oil supplies to the United States. The president can release the stored oil as necessary—including a release to stabilize prices. In addition to the SPR, there are also a Naval Petroleum Reserve and special emergency reserves of home heating oil maintained in storage tanks (some rented from commercial sources in other areas of the country).

The Strategic Petroleum Reserve (SPR) contains a mixture of oil from domestic and foreign sources.

The SPR is presently made up of four underground storage facilities located in salt domes along the coastal regions of Louisiana and Texas and has a total storage capacity of 700 million barrels of oil. These sites were chosen from among the more than 400 potential areas along the Gulf Coast of the southern United States after careful review of their relative geologic characteristics.

A salt dome is a body of rock salt surrounded by layers of sedimentary rock. Geologic characteristics considered in selecting storage sites include: 1) area geologic activity, 2) structural size, 3) existence of a trapping mechanism, 4) salt geometry, 5) salt composition, and 6) surface conditions.

Geologic activity in the area of potential storage sites must be well understood. The coastal plains along the Gulf Coast tend to be in a perpetual state of either subsidence or uplift and the rate of such relative change must be measurable and predictable.

Structural size is a significant factor. Oil is stored in cylindrically shaped caverns constructed within the salt body that are typically 200 feet in diameter and approximately 2,000 feet in height or larger. A storage dome may consist of from one to more than twenty caverns in a three-dimensional pattern. Salt domes along the Gulf Coast typically range between being one half to five miles in diameter and may be over 20,000 feet in vertical height.

Fluid naturally flows through permeable strata just as water passes through a sponge. Oil will seek the highest possible level due to its relatively low specific gravity and would float to the surface if not otherwise trapped. A salt dome must be overlain by a trapping mechanism in order to be an environmentally safe and an economically secure storage site, Cap rock is a stratum of rock lacking permeability that can act as a trapping mechanism. However, not all salt domes are overlain by cap rock.

Salt domes are usually formed as the lighter salt rises through sedimentary strata above in a plastic state from a deeper source while forming irregular shaped and sometimes freestanding columns. The three dimensional geometry of the salt diapir must be profiled in order to facilitate the design of the storage cavern pattern.

Ideally the salt dome is composed of homogenous halite free of shale or other sedimentary rock. The presence of irregularities in composition may effect cavern construction and containment integrity.

Surface conditions play a role in site selection and project design, construction and ease of operation. Typically such sites are located in marsh areas or beneath standing water. Proximity to existing infrastructure supporting oil import, delivery and water handling is a major cost and operational consideration.

Though geologically complex, salt domes have proven to be a reliably safe and economically competitive means of storing oil for future use and play a key role in national energy management and supply.

#### ■ FURTHER READING:

##### ELECTRONIC:

U.S. Department of Energy. "Fossil.Energy.gov Petroleum Reserves." <[http://www.fe.doe.gov/program\\_reserves.html](http://www.fe.doe.gov/program_reserves.html)> (March 2, 2003).

##### SEE ALSO

*DOE (United States Department of Energy) Petroleum Reserves, Determination*

## Stun Gun.

SEE *Less Lethal Weapons Technology*.

---

## Sudan, Intelligence and Security

---

Due to its role with connection to the international war on terrorism, Sudan has much greater importance in the realm of intelligence and security than do most nations of Africa's interior. Though it harbored al-Qaeda leader Osama bin Laden from 1991 to 1996, Sudan in 2001 became an unlikely ally of the United States in its efforts against Islamist terrorists.

The two principal intelligence agencies of the Sudanese government are Al Amn al-Dakhili and Al Amn al-Khariji, the bureaus of internal and external security respectively. Security issues in Sudan have, for the most part, sprung from internal issues, particularly a civil war with roots going back to the 1950s. The vast nation, Africa's largest geographically, is sharply divided culturally into northern and southern regions. The north, which

the government controls, is Arabic and Islamic, whereas the south is sub-Saharan African and non-Muslim (either Christian or traditionalist). The opposition Sudan People's Liberation Army (SPLA) controlled much of southern Sudan by the end of the twentieth century.

The Sudanese government has been notorious for its human rights violations, including the continuation of the black African slave trade in the 1990s. Its imposition of strict Muslim law on the south in 1983 sparked a civil war that claimed more than 1.5 million lives over the next 15 years. Meanwhile, the government in Khartoum provided safe haven to bin Laden, who had been exiled from his native Saudi Arabia. U.S. and Saudi pressure forced the Sudanese to eject bin Laden in 1996.

After the al-Qaeda attacks on U.S. embassies in Kenya and Tanzania in 1998, the U.S. military struck back at targets in Afghanistan and Sudan, whose Shifa Pharmaceutical Plant was reportedly making chemical weapons. In 2001, the *Financial Times* revealed that two months before the bombings, Sudanese external security bureau chief Gutbi al-Mahdi approached the regional head of the Federal Bureau of Investigation and offered to share intelligence on al-Qaeda. Suspicious of Khartoum, the administration of President William J. Clinton declined the offer.

The inauguration of President George W. Bush in 2001 signaled a change in U.S.-Sudanese relations. Even before the September 11 terrorist attacks, Sudanese intelligence had begun providing Washington with information on suspected terrorists who had resided in the country during the period 1991–96. Soon after the attacks, a senior State Department official told the *Washington Post* that Khartoum had made an "implicit" offer for the use of its military bases to strike against al-Qaeda. In March 2002, Sudanese authorities captured and imprisoned Anas Al-Liby, a senior al-Qaeda militant.

The Khartoum government made a peace deal with the SPLA in July 2002, and the two sides began work toward a ceasefire agreement.

#### ■ FURTHER READING:

##### PERIODICALS:

"Accused Al Qaeda Senior Militant Captured in Sudan." *Los Angeles Times*. (March 17, 2002): A20.

Alden, Edward, and Mark Turner. "Sudan's Surprise Deal with Rebels Catches Washington Off-Guard." *Financial Times*. (July 23, 2002): 10.

Huband, Mark. "U.S. Rejected Sudanese Files on al-Qaeda." *Financial Times*. (November 30, 2001): 1.

##### ELECTRONIC:

Sipress, Alan. "Sudan Provides Administration Intelligence on Bin Laden." *Wall Street Journal* (September 30, 2001): A14.

Sudan: Intelligence Agencies. Federation of American Scientists. <<http://www.fas.org/irp/world/sudan/index.html>> (March 1, 2003).

## SEE ALSO

*Egypt, Intelligence and Security*  
*Kenya, Bombing of United States Embassy*  
*Libya, Intelligence and Security*

---

## Suez Canal

---

As the longest canal in the world without locks, the Suez Canal links the Mediterranean and Red seas across the Isthmus of Suez. Although Egypt's ancient rulers devised a means of connecting the Nile River to the Red Sea, it was only in modern times that French engineer Ferdinand de Lesseps developed a workable design for the 101-mile (163-km) canal, which opened in 1869. In 1956, the canal became the site of an international crisis involving Britain, France, Egypt, and Israel. Today the canal remains a strategic point of movement of the world's oil supply.

**Early history.** From ancient times, trade flourished in the Mediterranean and Red Seas, and pharaohs recognized the advantage to be gained by connecting the two bodies. As early as 1500 b.c., pharaohs of Egypt's New Kingdom commissioned the building of a canal between the Nile and the Red Sea. This early canal was covered by sand, and though the late seventh century b.c. pharaoh Necho II attempted to build a new canal, the project would not be completed until the Persian invasion of Darius after 522 b.c. This canal eventually met the same fate as its predecessors, and successive rulers—the Greeks under Ptolemy I and Cleopatra, and later the Romans under Trajan—attempted to restore it, but in each case the canal fell into disrepair.

Napoleon Bonaparte, when he conquered Egypt in 1798, revived the idea of a canal, this one to directly connect the two seas. The project did not begin for half a century, however, due to engineers' misconceptions regarding relative water levels. Finally, Lesseps, the former French consul to Egypt, received a 99-year concession on the canal from the khedive of Egypt. With a crew of some 2.4 million Egyptian workers, he commenced the building project, which cost more than 125,000 lives over the course of a decade. The canal opened with much ceremony on November 17, 1869.

**Crisis and concerns.** Until the Suez Crisis of 1956, the Anglo-French Suez Canal Company controlled the canal. Egyptian president Gamal Abdel Nasser had developed increasingly close ties with the Communist bloc, and therefore, when he requested assistance in building the Aswan High Dam—a project intended to tame the Nile and provide hydroelectric power to Egypt—the United States, Britain, and France refused. On July 26, Nasser retaliated

by declaring martial law in the canal zone and seizing control of the canal.

Britain and France at first tried diplomacy, and when this failed, they sought Nasser's overthrow through an alliance with Israel. The three nations followed a classic "good cop/bad cop" strategy. On October 29, the Israelis invaded Egypt, whereupon Britain and France went into presented themselves as peacekeepers, and offered to occupy the canal zone on behalf of the United Nations (UN). Their actions raised such tensions among the two superpowers that both the United States and the Soviet Union very nearly intervened. The UN forced the evacuation of the French and British on December 22, and Israel pulled out in March 1957.

**Aftermath of the Suez Crisis.** The Suez Crisis raised the stature of Nasser immeasurably, and he has remained a powerful symbol to Arab nationalists such as Iraq's Saddam Hussein, the late Hafez al-Assad of Syria, and Libya's Muammar al-Qaddafi. The incident also marked the end of British and French influence in the Middle East, where they had held considerable sway for the better part of 150 years. From an intelligence standpoint, the Suez Crisis was significant for the role played by British interception of cipher transmissions, an operation known as Engulf.

Israel captured the Sinai Peninsula in the 1967 Arab-Israeli war, and for the next six years, the canal served as a buffer between Egypt and Israel. It was closed during that time, and the Egyptians, who regained control in 1973, only reopened it in 1975. Since then, they have widened it twice, and have plans to widen it again by 2010 so as to accommodate larger oil-carrying vessels. The U.S. Department of Energy has identified the Suez Canal as one of several geographic "chokepoints"—narrow passages that are both vital to the international oil trade and extremely susceptible to attacks or accidents.

### ■ FURTHER READING:

#### BOOKS:

- Immermann, Richard H. *John Foster Dulles and the Diplomacy of the Cold War*. Princeton, NJ: Princeton University Press, 1990.
- Kelly, Saul, and Anthony Gorst. *Whitehall and the Suez Crisis*. Portland, OR: Frank Cass, 2000.
- Kunz, Diane B. *The Economic Diplomacy of the Suez Crisis*. Chapel Hill: University of North Carolina Press, 1991.
- Kyle, Keith. *Suez*. New York: St. Martin's Press, 1991.

#### ELECTRONIC:

- World Oil Transit Chokepoints. U.S. Department of Energy. <<http://www.eia.doe.gov/emeu/cabs/choke.html>> (April 1, 2003).

#### SEE ALSO

*Egypt, Intelligence and Security*



*Engulf, Operation  
Israel, Intelligence and Security  
Middle East, Modern U.S. Security Policy and Interventions  
United Kingdom, Intelligence and Security*

## Suitcase Bombs.

SEE *Russian Nuclear Materials, Security Issues.*

---

## Supercomputers

---

■ BRIAN HOYLE

A supercomputer is a powerful computer that possesses the capacity to store and process far more information than is possible using a conventional personal computer.

An illustrative comparison can be made between the hard drive capacity of a personal computer and a supercomputer. Hard drive capacity is measured in terms of gigabytes. A gigabyte is one billion bytes. A byte is a unit of data that is eight binary digits (i.e., 0's and 1's) long; this is enough data to represent a number, letter, or a typographic symbol. Premium personal computers have a hard drive that is capable of storing on the order of 30 gigabytes of information. In contrast, a supercomputer has a capacity of 200 to 300 gigabytes or more.

Another useful comparison between supercomputers and personal computers is in the number of processors in each machine. A processor is the circuitry responsible for handling the instructions that drive a computer. Personal computers have a single processor. The largest supercomputers have thousands of processors.

This enormous computation power makes supercomputers capable of handling large amounts of data and processing information extremely quickly. For example, in April 2002, a Japanese supercomputer that contains 5,104 processors established a calculation speed record of 35,600 gigaflops (a gigaflop is one billion mathematical calculations per second). This exceeded the old record that was held by the ASCI White-Pacific supercomputer located at the Lawrence Livermore National Laboratory in Berkeley, California. The Livermore supercomputer, which is equipped with over 7,000 processors, achieves 7,226 gigaflops.

These speeds are a far cry from the first successful supercomputer, the Sage System CDC 6600, which was designed by Seymour Cray (founder of the Cray Corporation) in 1964. His computer had a speed of 9 megaflops, thousands of times slower than the present day versions. Still, at that time, the CDC 6600 was an impressive advance in computer technology.

Beginning around 1995, another approach to designing supercomputers appeared. In grid computing, thousands of individual computers are networked together,

even via the Internet. The combined computational power can exceed that of the all-in-one supercomputer at far less cost. In the grid approach, a problem can be broken down into components, and the components can be parceled out to the various computers. As the component problems are solved, the solutions are pieced back together mathematically to generate the overall solution.

The phenomenally fast calculation speeds of the present day supercomputers essentially corresponds to "real time," meaning an event can be monitored or analyzed as it occurs. For example, a detailed weather map, which would take a personal computer several days to compile, can be compiled on a supercomputer in just a few minutes.

Supercomputers like the Japanese version are built to model events such as climate change, global warming, and earthquake patterns. Increasingly, however, supercomputers are being used for security purposes such as the analysis of electronic transmissions (i.e., email, faxes, telephone calls) for codes. For example, a network of supercomputers and satellites that is called Echelon is used to monitor electronic communications in the United States, Canada, United Kingdom, Australia, and New Zealand. The stated purpose of Echelon is to combat terrorism and organized crime activities.

The next generation of supercomputers is under development. Three particularly promising technologies are being explored. The first of these is optical computing. Light is used instead of using electrons to carry information. Light moves much faster than an electron can, therefore the speed of transmission is greater.

The second technology is known as DNA computing. Here, recombining DNA in different sequences does calculations. The sequence(s) that are favored and persist represent the optimal solution. Solutions to problems can be deduced even before the problem has actually appeared.

The third technology is called quantum computing. Properties of atoms or nuclei, designated as quantum bits, or qubits, would be the computer's processor and memory. A quantum computer would be capable of doing a computation by working on many aspects of the problem at the same time, on many different numbers at once, then using these partial results to arrive at a single answer. For example, deciphering the correct code from a 400-digit number would take a supercomputer millions of years. However, a quantum computer that is about the size of a teacup could do the job in about a year.

### ■ FURTHER READING:

#### BOOKS:

Stork, David G. (ed) and Arthur C. Clarke. *HAL's Legacy: 2001's Computer Dream and Reality*. Boston: MIT Press, 1998.

#### ELECTRONIC:

Cray Corporation. "What Is a Supercomputer?" Supercomputing. 2002. <<http://www.cray.com/supercomputing>>(15 December 2002).



A technician monitors IBM's ASCI White in 2000, then the world's fastest supercomputer, that is capable of 12 trillion calculations per second. The Department of Energy uses ASCI White to analyze and protect the nation's nuclear weapons stockpile. AP/WIDE WORLD PHOTOS.

The History of Computing Foundation. "Introduction to Supercomputers." Supercomputers. October 13, 2002. <<http://www.thocp.net/hardware/supercomputers.htm>>(15 December 2002).

**SEE ALSO**

*Computer Hardware Security*  
*Information Warfare*

---

## Surgeon General and Nuclear, Biological, and Chemical Defense, United States Office

---

Among its many responsibilities, the Office of the United States Surgeon General serves as a clearinghouse for

information on what is known as "medical NBC"—that is, the biomedical effects of nuclear, biological, and chemical (NBC) weapons and agents. Through the World Wide Web, the Surgeon General's office keeps physicians, as well as the general public, informed of dangers associated with anthrax, weapons of mass destruction, and other threats that became a part of public discourse after the terrorist attacks of September, 2001 and the subsequent war on terror.

The Office of the Surgeon General of the United States dates back to 1871, when President Ulysses S. Grant established the position. Appointed by the President with the advice and consent of the U.S. Senate, the Surgeon General serves a four-year term and reports to the Assistant Secretary for Health, principal advisor to the Secretary of Health and Human Services (HHS) on public health and scientific issues. The Surgeon General holds the rank of vice admiral in the U.S. Public Health Service Commissioned Corps, a uniformed service.

The Surgeon General Medical NBC Server was established after September 2001, to provide a reference and learning source on medical NBC matters. Although it is directed toward physicians, much of the information on the site (<http://www.nbc-med.org>) is accessible to citizens without medical training. The site was intended to supplement the Army Medical Department Center and School Distance Learning effort, and to coordinate with existing initiatives to provide Internet access to all medical facilities, both stationary and in the field. The Medical NBC Server also provides health advisories from groups that include the Food and Drug Administration, HHS, and even the U.S. Postal Service.

#### ■ FURTHER READING:

##### ELECTRONIC:

Medical NBC Online Information Server. <<http://www.nbc-med.org/>> (April 2, 2003).

Office of the Surgeon General. <<http://www.surgeon-general.gov/>> (April 2, 2003).

##### SEE ALSO

*Anthrax, Terrorist Use as a Biological Weapon*  
*Biological Warfare*  
*Biological Warfare, Advanced Diagnostics*  
*CDC (United States Centers for Disease Control and Prevention)*  
*Public Health Service (PHS), United States*  
*USAMRICD (United States Army Medical Research Institute of Chemical Defense)*  
*USAMRIID (United States Army Medical Research Institute of Infectious Diseases)*  
*Weapons of Mass Destruction*

---

## Sweden, Intelligence and Security

---

Sweden established its national intelligence services in 1937, in response to escalating political and military tensions in Europe and the rise of Nazi Germany. While the Swedish military had maintained a unit of trained espionage and counterespionage agents since the early nineteenth century, the nation lacked a modern and specialized intelligence force. The initial intelligence services consisted of a central intelligence agency, a cryptology department, and a signals intelligence department.

Sweden's cryptology department, despite rudimentary equipment, quickly gained fame. In cooperation with

the the signals intelligence department and the Navy, Swedish intelligence intercepted and deciphered nearly half of all German radio and wire transmissions in the years immediately preceding World War II. During the War, Nazi Germany considered Sweden's cryptology department one of its primary security threats. Sweden's intelligence services and cryptologists worked closely with some Allied forces, and in the early war years, provided key information to British cryptologists at Bletchley Park.

After the war, Sweden's geographic location made it a useful station for monitoring Eastern Europe and the Soviet Union during the Cold War. Today, Sweden is a member of the European Union and contributes signals intelligence, as well as cryptological technology, to European cooperative intelligence operations. Though the country has a stated policy of neutrality, Sweden maintains one of Europe's largest and best-equipped intelligence forces.

The Swedish intelligence community does not use the traditional internal and external intelligence divisions within its various branches. Though operational units may be more specialized, military and civilian intelligence and security forces in Sweden collect both internal and foreign data. Government and military agencies often coordinate operations, especially in the areas of signals and counter-intelligence.

The Military Intelligence and Security Directorate (MUST) oversees Swedish military intelligence operations. The agency coordinates intelligence operations with various specialized military units. The Special Protection Group (SSG) is the military's highly trained intelligence and special forces unit. The SSG protects intelligence and military installations. A Military Police division, with a specially trained covert operations unit called the Military Police Rangers (MPJ), is charged with the protection of military property and defense of national security.

The National Security Service (SAPO) is Sweden's primary government intelligence service. SAPO directs maintains several operational branches, including signals intelligence, counterintelligence, and a national police force. The agency oversees and both foreign and domestic surveillance and analyzes intelligence data. The national police force is the main action unit of the SAPO, and maintains important operational divisions of its own, including the ONI, the Swedish national police counter-terrorism unit. The unit has special operational and military action powers to seek out and apprehend terrorists inside Sweden's borders and throughout Europe, with the aid of foreign intelligence agencies.

In response to growing concern about global terrorism, Sweden joined the European Union international task force to combat terrorism.

##### SEE ALSO

*European Union*  
*Counter-Intelligence*

## Switzerland, Intelligence and Security

Switzerland has a long tradition of neutrality, abstaining from active participation in World Wars I and II. This policy of neutrality extended to abstaining from membership in international organizations and prohibiting the sharing of some intelligence information with foreign nations. On September 10, 2002, the Swiss Confederation joined the United Nations as a member nation, ending a fifty-five year span as an observer mission. Although Switzerland has cooperated with humanitarian, economic, legal, and intelligence operations with neighboring foreign nations and the United States, it is not a member of the European Union or the North Atlantic Treaty Organization (NATO).

Swiss government agencies, financial institutions, and military branches of service recognize three national languages, German, French, and Italian. Some canton governments use a fourth national language, Romansh. The varied linguistic ethnicities in the country require national services to operate equally in all of its official languages. The multi-lingual nature of the Swiss Confederation and its citizens adds a unique dimension to Swiss intelligence and security forces.

Switzerland's intelligence services effectively dissolved intelligence community distinctions between internal and domestic security and intelligence operations. The recent creation of the Swiss National Security Council, part of the Swiss Federal Department of Defense, Civil Protection, and Sports, facilitated communication and cooperation among various agencies in the intelligence community, giving each independent agency equal access to information and resources. The National Security Council has jurisdiction over civilian and military intelligence and security issues, further uniting various branches of the intelligence community.

The Strategic Intelligence Service is charged with directing and conducting foreign intelligence operations. Its charge is the protection of Swiss banking, economic, political, technological, and military interests abroad. Data collected by the agency is reported to the political and military leadership of the Swiss Confederation via the National Security Council. The Strategic Intelligence Service traditionally works in conjunction with other Swiss agencies, but has increasingly cooperated with adjacent nations in the European Union.

The Armed Forces Intelligence Service trains most Swiss intelligence agents. The agency provides military intelligence units should the army be needed in domestic affairs or called to active duty. Within the armed forces, political and security information is gathered by the Air Force Intelligence Section which conducts internal surveillance of the Swiss intelligence community.

Switzerland's most populous agency in the intelligence community is the Federal Office of Police. The Federal Police are Switzerland's main counterintelligence force, conducting both internal and external surveillance. The Federal Office of Police works closely with other agencies to ensure domestic security.

## Syria, Intelligence and Security

Syria has four intelligence agencies, which together helped President Hafez al-Assad maintain strict control of the nation from 1970 to 2000, and assisted the transition of power to his son Bashar after the elder Assad died. Despite the country's reputation as a police state and an exporter of terrorism within the Middle East, Syrian opposition to Iraq and to Islamist groups has often placed it in temporary alignment with United States policies.

The Political Security Directorate (Idarat al-Amn al-Siyasi) conducts surveillance within the country, looking for signs of opposition political activity. Its role overlaps to some extent that of the General Security (or Intelligence) Directorate (Idarat al-Amn al-'Amm), the principal civilian intelligence agency in the country. The latter also has an external security division equivalent to the U.S. Central Intelligence Agency, as well as a Palestine division, which oversees activities of Palestinian groups in Syria and Lebanon.

In addition to the typical functions of military intelligence, the Military Intelligence Service (Shu'bat al-Mukhabarat al-'Askariyya) provides support to Palestinian, Lebanese, and Turkish radical groups, monitors Syrian dissidents living overseas, and coordinates the actions of Syrian and Lebanese forces in Lebanon.

The fourth intelligence service, the Air Force Intelligence Directorate (Idarat al-Mukhabarat al-Jawiiyya) is only nominally tied to the air force. Its role as the most powerful and feared intelligence agency in Syria comes from the fact that Hafez al-Assad was once air force commander, and later turned the air force intelligence service into his personal action bureau. In addition to intelligence work, the directorate has assisted numerous terrorist operations abroad.

Despite its reputation, Syria has made common cause with the United States against Iraq, whose Saddam Hussein was a hated foe of Assad, and against militant Islamists. After the U.S. defeat of the Taliban in Afghanistan, extremists ejected from that country began to drift through Syria, but found themselves unwelcome there: the Syrians captured numerous former fighters and held them for questioning by U.S. authorities. In July 2002, U.S. officials

confirmed that Syria's government had provided Washington with information that helped head off a surprise attack on U.S. forces in the Persian Gulf.

■ FURTHER READING:

BOOKS:

Bennett, Richard M. *Espionage: An Encyclopedia of Spies and Secrets*. London: Virgin Books, 2002.

PERIODICALS:

Boyne, Sean. "Assad Purges Security Chiefs to Smooth the Way for Succession." *Jane's Intelligence Review* 11, no. 6 (June 1, 1999): 1.

Schneider, Howard. "Syria Evolves as Anti-Terror Ally." *Washington Post*. (July 25, 2002): A18.

ELECTRONIC:

Syria: Intelligence Agencies. Federation of American Scientists. <<http://www.fas.org/irp/world/syria/>> (March 1, 2003).

Syria's Intelligence Services: A Primer. Middle East Intelligence Bulletin <[http://www.meib.org/articles/0007\\_s3.htm](http://www.meib.org/articles/0007_s3.htm)> (March 1, 2003).

SEE ALSO

*Iraq, Intelligence and Security Agencies*  
*Israel, Intelligence and Security*  
*Jordan, Intelligence and Security*  
*Turkey, Intelligence and Security*



## Tabun

Tabun (or “GA”) is one of a group of synthetic chemicals that were developed in Germany during the 1930s and 1940s (Tabun was developed in 1936). The original intent of these compounds, including tabun, was to control insects. These pesticides were similar to organophosphates in their action on the nervous system. However, Tabun and the other human-made nerve agents proved to be much more potent than the organophosphates, and so quickly became attractive as chemical weapons.

Tabun is one of the G-type nerve agents, along with Sarin and Soman. They are all clear, colorless, and tasteless. As a result, Tabun mixes readily with water, and so can be used as a water-poisoning agent. Food can also be contaminated. The fluid form of Tabun can also be absorbed through the skin.

When in water, Tabun loses its potency relatively quickly, compared to airborne vapors, which can remain potent for a few days. The vapors can even bind to clothing, where they will subsequently be released for 30 minutes or so. People close to the contaminated person can themselves be affected by the vapor. Tabun vapors tend to be denser than air and so settle into low-lying depressions or valleys. People in such regions are especially susceptible.

Like the other members of the G series, Tabun is a nerve agent. Specifically, it inhibits an enzyme called cholinesterase. The enzyme breaks apart a compound that acts as a communication bridge between adjacent nerve cells. Normally, the transient formation and destruction of the bridge allows a control over the transmission of nerve impulses. But, the permanent presence of the bridging compound means that nerves “fire” constantly, which causes muscles to tire and eventually stop functioning. In the case of the lungs, this can be fatal.

Symptoms of Tabun poisoning, which can begin within minutes of exposure, include runny nose, watery and painful eyes, drooling, excessive sweating, rapid breathing, heart beat abnormalities, and, in severe cases, convulsions, paralysis, and even fatal respiratory failure.

Treatment for the inhalation of Tabun consists of three timed injections of a nerve agent antidote such as atropine. Since this may or may not be successful, prevention remains the most prudent strategy. Protective clothing including a gas mask is a wise precaution for those who are in an environment where the deployment of Tabun is suspected.

While the United States once had an active chemical weapons development program that included the weaponization of Tabun, this program was halted decades ago. Other countries may still be engaged in such weapons development. For example, Iraq is suspected of having used Tabun against Iranians during the Iran-Iraq war in the 1980s.

### ■ FURTHER READING :

#### BOOKS:

Government of the United States. *21st Century Complete Guide to Chemical Weapons and Chemical Terrorism—U.S. Demilitarization Program, Stockpile Destruction Emergency Plans, Nerve Gas and Blister Agent Civilian Treatment and First Aid, Home Sheltering Plans*. Washington, DC: Progressive Management, 2002.

#### ELECTRONIC:

Agency for Toxic Substances and Disease Registry. “Nerve Agents (GA, GB, GD, VX).” Division of Toxicology, Centers for Disease Control and Prevention. March 13, 2003. <<http://www.atsdr.cdc.gov/tfactsd4.html>>(April 10, 2003).

Agency for Toxic Substances and Disease Registry. “Facts about Tabun.” Division of Toxicology, Centers for Disease Control and Prevention. March 7, 2003. <<http://www.bt.cdc.gov/agent/tabun/basics/facts.asp>>(April 10, 2003).

## SEE ALSO

*Chemical Warfare*  
*Mustard Gas*  
*Sarin Gas*

## Taiwan, Intelligence and Security

For the first four decades after its establishment by ousted Chinese President Chiang Kai-shek in the 1940s, the Republic of China (ROC) or Taiwan was a virtual one-party state ruled by Chiang's Guomindang or KMT. Although its system was capitalist and nominally democratic, the country's people had little freedom of dissent. During those years, the National Security Bureau (NSB) helped maintain Chiang's power by monitoring the citizenry. Liberalization began in the late 1980s, and was reflected in changes by the NSB. Nevertheless, the centralization of the ROC intelligence and security structure remains.

Under the National Security Council (NSC) is the Ministry of Defense, which includes the ROC Army, Navy, Air Force, Coast Guard, and Military Police Command. The Ministry of Defense also has its own Military Intelligence Bureau. Of much greater significance in the intelligence apparatus is NSB, which reports directly to the Ministry of Defense. At one time, its activities were so secretive that it was called "Mystical 110," after the address of its headquarters at 110 Yanteh Boulevard in the Taipei suburb of Yang Ming Mountain. Directed by military leaders, the NSB was known popularly as "Taiwan's KGB" or simply "TKGB." The passage of the NSB Organic Law by the Yuan or national legislature in 1994, however, served to place NSB under a much greater measure of civilian control in the increasingly liberalizing ROC state.

In addition to the NSB is the Ministry of Justice Investigation Bureau (MJIB), which performs functions similar to those of the United States Federal Bureau of Investigation, although its powers are somewhat more broad. Police services are directed by the National Police Administration of the Ministry of Interior. Like South Korea and unlike the United States, Taiwan's police are centrally organized.

### ■ FURTHER READING:

#### BOOKS:

Bennett, Richard M. *Espionage: An Encyclopedia of Spies and Secrets*. London: Virgin Books, 2002.

#### PERIODICALS:

Campbell, Kurt M. "Edging Taiwan in from the Cold." *Washington Post*. (April 25, 2001): A31.

Dean, Jason. "Taipei's Turmoil Hinders Action on Key Issues." *Wall Street Journal*. (March 21, 2002): A18.

Li Shaomin. "My Long Journey Home." *Wall Street Journal*. (August 7, 2001): A14.

#### ELECTRONIC:

Taiwan Intelligence and Security Agencies. Federation of American Scientists. <<http://www.fas.org/irp/world/taiwan/>> (March 1, 2003).

#### SEE ALSO

*China, Intelligence and Security*  
*Chinese Espionage against the United States*  
*South Korea, Intelligence and Security*

## Taser

■ BRIAN HOYLE

A Taser is a type of gun. It is similar in appearance to a conventional gun, having a handle, squeezable trigger, and a blunt barrel. Instead of firing bullets, however, a Taser incapacitates someone for a short time by the use of electricity. Tasers are most often used by security forces, including police, to quell disturbances without causing injury to the people involved.

The Taser gun is one of three types of weapons that are known collectively as stun guns. The other two devices are known as the hand held stun gun and the liquid stun gun. As their name implies, these weapons are designed to be a non-lethal defense, rather than an offensive weapon capable of causing deadly injury.

Stun guns like the Taser operate by disrupting the electrical flow of signals through nerve cells. This electrical flow drives the ability of the muscles to respond to commands from the brain, and allows information that the body receives from the outside world (i.e., touch, taste, smell) to be communicated to the brain. The disruption of the nerve cells is achieved by the generation of an electrical charge by the Taser that has a high voltage and low amperage. Put another way, the electrical charge has a great deal of pressure, but is not intense. The pressure of the charge allows the charge to penetrate into the body, even though several layers of clothing. In order for it to be effective, the person must be close, even in direct contact, with the electrodes of the Taser. Because the electrical charge is not intense, the brief surge of electricity is not powerful enough to physically damage the person's body.

Inside the body, however, the electricity is powerful enough to temporarily disable the nervous system. This occurs when the added charge mixes with the electrical impulses flowing through the nerve cells. The added electricity overwhelms the meaningful signals, making it impossible for the brain to interpret the signals from the



An advanced M-26 Taser stun gun is demonstrated during a news conference in 2002. Several airlines deploy similar weapons on board during flights. AP/WIDE WORLD PHOTOS.

nerve cells. Confusion, difficulty in balance, and muscle paralysis results.

Only about one-quarter of a second is required to incapacitate someone. Once the electrical swamping of the nerve impulses has abated—within a few seconds to a minute—recovery is complete with no adverse effects. Tests have shown that even heart pacemakers are not affected by Tasers.

The electrical signal from a Taser can be generated as a single burst, or in rapid pulses. If the pulses are similar to the frequency of the natural pulses that occur within the nerve cells, then the muscles are stimulated to contract and relax. However, there is no coordination behind the work, since the connections between the muscles and the brain have been disrupted. The muscles will become depleted of energy and tired. Even when the normal electrical rhythm is restored, the muscles often remain too tired to respond for a short period.

Because a Taser acts on muscles, and as there are muscles all over the body, a Taser applied almost anywhere over the body can cause total immobilization.

Stun guns, including the Taser, consist of a transformer, oscillator, capacitor, and electrodes. The transformer generates the voltage; typically between 20,000 and 150,000 volts. The oscillator introduces the pulsations in the electrical charge. The charge is built up in the

capacitor, which releases the charge to the electrodes. It is the electrodes that send the charge into the body, when the electricity bridges the gap between the oppositely charged electrodes.

In a Taser, the electrodes are not fixed in position. Instead, they are positioned on the ends of two long pieces of conducting wire. When a trigger is pulled, a release of compressed gas expels the electrodes out from the gun. In addition, the electrodes have barbs on them, so that they can stick to clothing. This design of the Taser allows a charge to be transferred to someone who is 15 to 20 feet away. Hand-to-hand contact, in this instance, is not necessary. The disadvantage of this design is that only one shot is possible before the electrodes have to rewind, and a new compressed gas cartridge loaded into the gun. Some models of Taser have the attached electrodes, so that if the flying electrodes miss the target, the shooter can move in and try to touch the subject with the stationary electrodes to deliver the stunning dose of electricity.

#### ■ FURTHER READING:

##### BOOKS:

Murray, John, James H. Murray, and Barnet Resnick. *A Guide to Taser Technology: Stunguns, Lies, and Videotape*. Dana Point: Whitewater Press, 1997.



**ELECTRONIC:**

How Stuff Works. "How Stun Guns Work." <<http://www.howstuffworks.com/stun-gun.htm>> (16 December 2002).

**SEE ALSO**

*Electromagnetic Weapons, Biochemical Effects  
Energy Directed Weapons  
Less Lethal Weapons Technology*

Polmar, Norman, and Thomas B. Allen. *Spy Book: The Encyclopedia of Espionage*. New York: Random House, 1998.

*Scientists and Engineers: Directorate for Scientific and Technical Intelligence, Directorate for Foreign Intelligence*. Washington, D.C.: Defense Intelligence Agency, 1987.

**ELECTRONIC:**

Army Technical Intelligence Chronology. University of Idaho Library. <<http://www.lib.uidaho.edu/technical/tech-int.html>> (April 3, 2003).

**SEE ALSO**

*Chinese Espionage against the United States  
IMINT (Imagery intelligence)  
Measurement and Signatures Intelligence (MASINT)  
Sabotage  
Satellite Technology Exports to the People's Republic of China (PRC)  
SIGINT (Signals Intelligence)*

---

## Technical Intelligence

---

Technical intelligence, or TECHINT, is intelligence relating to the technical abilities of an enemy. It does not fall under just one of the four major branches of intelligence; rather, TECHINT includes elements of imagery, measurement and signatures, and signals intelligence (IMINT, MASINT, and SIGINT, respectively). It may also intersect with the fourth major branch, human intelligence (HUMINT), though some adherents of TECHINT insist that HUMINT plays no part in the gathering of technical intelligence. Closely related to TECHINT is scientific intelligence, or intelligence on the development of new weapons or techniques by an enemy.

Both sides in World War II conducted technical and scientific intelligence operations against one another. For example, the British followed a supply of heavy water, to be used by the Nazis in building an atomic bomb, for several years, and finally destroyed it in transit from Norway to Germany.

Technical and scientific intelligence operations proliferated during the Cold War, along with the many scientific advances that made possible improvements in weapons and surveillance technology. The most notable TECHINT operations were conducted by the Soviets against the United States, as when Julius and Ethel Rosenberg, agents of the Soviet regime, passed nuclear secrets to Moscow.

Much of the reason for the lopsided character of Cold War TECHINT (with the exception of the early space race) was the fact that the United States had far more military and commercial technical expertise to offer than did the Soviet Union. An even greater disparity existed between the United States and the People's Republic of China (PRC) at the end of the twentieth century, when PRC operatives sought to obtain information on U.S. weapons systems and satellites. Much of this material came not as a result of espionage operations, but through open sources.

**■ FURTHER READING:**

**BOOKS:**

Chalou, George C. *Scientific and Technical Intelligence Gathering*. New York: Garland Publishing, 1989.

---

## Technology Transfer Center (NTTC), Emergency Response Technology Program

---

The National Technology Transfer Center (NTTC) is a research facility on the campus of Wheeling Jesuit University in Wheeling, West Virginia. It was established by Congress in 1989, with a mandate to increase the effectiveness of U.S. industry by providing access to some \$70 billion in federally funded research. Among the facilities of this full-service technology management and commercialization center is the Emergency Response Technology (ERT) Program. The latter attempts to match the technology needs of emergency medical, firefighting, hazardous materials, public safety, and special operations personnel with off-the-shelf technologies.

The ERT Program is led by its advisory council, the Emergency Response Technology Group (ERTG). It is the responsibility of the ERTG to identify technology needs and match them to a range of existing technologies. Those existing technologies are evaluated with regard to their applicability to specific areas of need, and assuming it meets the test, the technology is brought before the ERTG as a group to validate it. Upon validating, the ERTG undertakes assistance of the developer by overseeing operational tests and evaluations at participating facilities throughout the United States. Once successfully brought to market, what was once a prototype becomes an operational commercial product.

Among the products the ERTG sought to develop in 2003 was a building and facility emergency response

information/survey tool, which would store data, including location of power panels and wiring, to enhance the ability of rescue personnel to penetrate all areas of a building; a personnel locator/monitor that would provide three-dimensional tracking of emergency personnel at an emergency site; an approaching traffic warning device; and a hazard assessment robot that could be passively activated by remote sensors. In the 18 months prior to September 2002, according to the *Chronicle of Higher Education*, the NTTC as a whole had brokered some 30 deals in which business firms licensed technology developed by the National Aeronautics and Space Administration and the Environmental Protection Agency. An example of a product it had recently helped market was the RoadSpike, a portable device capable of deflating tires of motorists attempting to run roadblocks.

#### ■ FURTHER READING:

##### PERIODICALS:

Brainard, Jeffrey. "Profiles in Pork: Wheeling Jesuit University: National Technology Transfer Center." *The Chronicle of Higher Education* 49, no. 5 (September 27, 2002): A23.

Ritchie-Matsumoto, Peggy. "Taking Your Technology to the Marketplace." *Corrections Today* 62, no. 4 (July 2000): 96–100.

##### ELECTRONIC:

National Technology Transfer Center. <<http://www.nttc.edu>> (March 18, 2003).

##### SEE ALSO

*Chemical Safety: Emergency Responses*  
*Law Enforcement, Responses to Terrorism*  
*Radiological Emergency Response Plan, United States Federal*

---

## Telemetry

---

Telemetry, from the Greek *tele* (far) and *metron* (measure), is the collection of data using automated sensors that transmit their results to a central monitoring point. A telemetric sensor may be stationary (e.g., fixed on the sea floor) or aboard a mobile platform (e.g., airplane, spacecraft, missile, submarine). The quantities sensed are usually simple variables that can be reported at regular intervals, such as temperature, pressure, humidity, altitude, fuel level, battery voltage, salinity, vibrational intensity, alarm status, or the like. Complex, high-speed signals such as video are usually not termed telemetry, even when they are collected remotely by unattended devices.

The raw output of a remote sensor is often an analog signal, that is, a voltage or current that varies smoothly

with time. Before transmission, such a signal is usually converted to digital form by the process of analog-to-digital conversion or sampling. In sampling, an analog signal is examined at evenly-spaced moments and a binary number assigned to its magnitude; the larger the sensor output, the larger the binary number. The raw bitstream produced by sampling is organized by the telemetry device into standard-length frames containing added information specifying data type, time of acquisition, and so forth. If the transmission channel is noisy, the signal may also be subjected to error-correction coding to allow recovery of data from errors. The signal may also, in some military applications, be encrypted before transmission. The final telemetry signal is sent from the data-collection point using radio, sonar, coaxial cable, or some other medium to a receiving station, where it is recorded and monitored by computers or human operators.

Telemetry is employed for many purposes throughout the commercial, scientific, and military sectors. For example, controllers of missiles, torpedoes, spacecraft, or remotely piloted aircraft such as the Predator require access to numerical information of many sorts in order to monitor and adjust the performance of these complex machines. Telemetric data may also be used for surveillance purposes, as when deep-sea acoustic sensors are used to track submarine movements, and is essential to the control of spacecraft, whether crewed or robotic.

#### ■ FURTHER READING:

##### ELECTRONIC:

Wilson, Elizabeth. *Introduction to AMMOS Telemetry Processing*. Jet Propulsion Laboratory, NASA. October 18, 2001. <<http://tel.jpl.nasa.gov/~betsy/mm/intro.htm>> (Nov. 14, 2002).

##### SEE ALSO

*Cipher Pad*  
*Codes and Ciphers*

---

## Telephone Caller Identification (Caller ID)

---

Caller identification, or caller ID, permits the receiver of a call to identify the caller's location. Available since the early 1990s, it has enhanced the sense of privacy enjoyed by persons in their homes, and has also greatly reduced the number of prank calls, as well as calls made with threatening or criminal intent. Ambivalence about the privacy ramifications of caller ID, however, has made the state of California slow to accept the technology.

In 1985, the *Los Angeles Times* ran a report on an ultra-chic security products boutique whose customers included the late Shah of Iran and the makers of the James Bond movies. Counter Spy Shop (CSS) in Washington, D.C., sold a telephone voice scrambler for \$14,000, yet, as the newspaper article noted, "What CSS cannot do, despite numerous requests from potential customers, is pinpoint the place of origin of an incoming call." To do so "would require access to the telephone company's computers, something that even CSS lacks."

Within half a decade, telephone companies had made such technology available, for a small fee, to all customers. A caller ID box, or a caller ID unit built into a phone, simply reads the computerized information for the incoming call, assuming it is coming from a listed number. Calls from an unlisted number register as "Unknown Caller" or "Private Caller." Available on internal private branch exchange (PBX) telephone systems during the 1980s, caller ID gained use by businesses offering toll-free numbers in 1988. It became available to residential customers in 1989, and by 2001, 43% of homes nationwide had caller ID.

An exception was California, where privacy concerns had kept the service away for many years. Before telephone companies could bring caller ID into the state, they had to spend \$34 million on an advertising campaign to tell callers that the service would make their phone numbers visible, and that this could be used to obtain the caller's address. By 2001, four years after the introduction of caller ID in the state, about one quarter of Californians used the service.

#### ■ FURTHER READING:

##### PERIODICALS:

- Crabb, Peter B. "The Use of Answering Machines and Caller ID to Regulate Home Privacy." *Environment and Behavior* 31, no. 5 (September 1999): 657–70.
- Kupperschmid, David. "James Bond 'Supplier' Has the Cure for Whatever Is Bugging You." *Los Angeles Times*. (April 26, 1985): 2.
- MacSweeney, Greg. "Caller ID with a Kick." *Insurance & Technology* 25, no. 10 (October 2000): 30–35.
- Mehta, Stephanie N. "Playing Hide-and-Seek by Telephone—Phone Companies Are Arming Both Sides in the Battle to Screen Unwanted Callers." *Wall Street Journal*. (December 13, 1999): B1.
- "Tech 101: Hollywood's Caller ID Hang-Up." *Los Angeles Times*. (May 24, 2001): T1.

##### ELECTRONIC:

- Johnson, Jeff. Caller Identification: More Privacy or Less?—Winter-Spring 1990 (Volume 8, Number 2). Computer Professionals for Social Responsibility. <<http://www.cpsr.org/publications/newsletters/issues/2001/summer/jj.html>> (April 2, 2003).

#### SEE ALSO

*Privacy: Legal and Ethical Issues*  
*Telephone Scrambler*

## Telephone Recording Laws

In the United States, each state has its own laws regarding the recording of phone calls, while recording of interstate calls is governed by federal law, most notably the Federal Wiretapping Act. In some cases, taping is legal with the consent of both parties, but the laws can be complex and open to arcane interpretations. Recording of conversations has played an important role in American political and legal history, from Watergate and other presidential scandals to lesser-known cases.

President Richard M. Nixon's illegal taping of private conversations figured prominently in the Watergate scandal of the early 1970s, although in fact, presidents have been recording conversations for as long as such technology has been available. In the Clinton-Lewinsky scandal, involving President William J. Clinton's sexual relationship with White House intern Monica Lewinsky and his attempts to cover it up, key evidence came from conversations between Lewinsky and her friend Linda Tripp—conversations Tripp recorded without telling Lewinsky. Such was the depth of Americans' resentment toward the threat of privacy invasion (combined with popular liking for the affable Clinton) that Tripp become the focus of far greater condemnation than did the President.

In 1997, secretly made tapes of Texaco executives furnished proof of racial discrimination, and led the company to settle a \$176 million lawsuit.

Although Justice Louis Brandeis described wiretapping as "evil" in *Olmstead v. United States* (1928; 277 U.S. 438), the federal government has, in the view of many civil liberties groups, at best a questionable record in this area. Since the 1970s, a backlash against domestic surveillance and intelligence efforts has reduced the power of the Federal Bureau of Investigation and other law-enforcement authorities in this area. As for telephone recording by individuals, this is subject to some form of criminal penalty in all 50 states, and at the federal level. However, the Federal Wiretapping Act does allow telephone service providers, business owners, and consenting parties to record calls under certain circumstances.

#### ■ FURTHER READING:

##### PERIODICALS:

- Cloud, David S., and David Rogers. "Telecom Firms Lobby for Funding of Upgrades to Ease Surveillance." *Wall Street Journal*. (April 5, 2000): A4.
- Halbfinger, David M. "Mother and Lawyer Charged in Sale of 10-Week Old Baby." *New York Times*. (March 30, 1999): 4.
- McCarter, Kimberly M. "Tape Recording Interviews." *Marketing Research* 8, no. 3 (fall 1996): 50–51.
- Skoning, Gerald. "Be Careful Not to 'Tripp'." *HR Magazine* 43, no. 6 (May 1998): 125–30.

## SEE ALSO

*Domestic Intelligence*  
*Foreign Intelligence Surveillance Court of Review*  
*Privacy: Legal and Ethical Issues*  
*Telephone Recording System*  
*Telephone Tap Detector*

## Telephone Recording System

A telephone recording system can be as simple as a handheld phone receiver with an analogue (non-computerized, non-digital) recorder. In such a situation, the act of recording is hard to hide. On the other hand, some telephone recording systems are so seamless that the individual being recorded would not know unless informed. For this reason, some states require that the person being recorded be informed of this fact, and many states require that the recorder emit a regular beep or other sound to serve as a reminder of the ongoing recording.

Consumers today are able to buy telephone recording systems that hook into the telephone line just as an answering machine would. Such systems, which retail from under \$100, make it possible to begin recording as soon as the receiver is lifted. Twelve states require "two-party notification," meaning that both participants in a recorded conversation must be informed of the fact that they are being recorded.

In California, laws further require that the recording equipment continually emit a beeping tone so as to maintain awareness of the recording process. Sophisticated consumer recording systems can be configured in such a way as to play the beep if necessary. Digital systems are even capable of saving a recorded call in a digital audio format, as a .wav file, making it possible for a user to e-mail a recording of a conversation.

### ■ FURTHER READING:

#### PERIODICALS:

- Cloud, David S., and David Rogers. "Telecom Firms Lobby for Funding of Upgrades to Ease Surveillance." *Wall Street Journal*. (April 5, 2000): A4.
- McCarter, Kimberly M. "Tape Recording Interviews." *Marketing Research* 8, no. 3 (Fall 1996): 50–51.
- Skoning, Gerald. "Be Careful Not to 'Tripp'." *HR Magazine* 43, no. 6 (May 1998): 125–130.

## SEE ALSO

*Domestic Intelligence*  
*Privacy: Legal and Ethical Issues*

*Telephone Recording Laws*  
*Telephone Tap Detector*

## Telephone Scrambler

A telephone scrambler encrypts phone conversations, keeping unauthorized users from tapping into or monitoring calls with any success. Scrambling involves the encryption of data, using unique codes that render it possible only for authorized personnel to unscramble transmissions. In order for scrambling technology to work, it is necessary that both authorized participants in a conversation possess a scrambler/descrambler. Scramblers are available on the consumer market, but most of these are vastly inferior to the technology used by operatives of elite U.S. intelligence services.

In a phone scrambling system, information sent over a public switched telephone network, or PSTN, is scrambled. The authentication of the unscrambling device at the receiving end is checked, and when an incoming message is received, it remains inaccessible until a special code or identification number is entered. One consumer system, according to a report in the trade journal *Security*, uses voice coding technology as a further security measure.

The principle of telephone scrambling is similar to that applied in making a Web site secure so that users can enter financial information without fear that this data will be intercepted. In both cases, sophisticated encryption makes it all but impossible for interlopers to obtain the desired information.

It is a safe bet that decryption technology and techniques available to an upper-echelon intelligence organization such as the National Security Agency, on the other hand, could easily break into even the best civilian systems. Likewise, U.S. intelligence services in hostile environments such as Iraq during the 2003 war have at their disposal telephone scrambling and decryption technology that would make their transmissions virtually impenetrable.

### ■ FURTHER READING:

#### PERIODICALS:

- Baldauf, Scott. "Where to Find the Perfect Gift for Your 007 Wannabe." *Christian Science Monitor*. (December 7, 1999): 2.
- "How Secure Are Your Phone, Fax, Data Transmission Systems?" *Security* 34, no. 6 (June 1997): 75–76.
- Nolte, Carl. "Spy Store a Boon for Paranoid Public." *San Francisco Chronicle*. (January 18, 2002): A23.

## SEE ALSO

*Domestic Intelligence*

*Encryption of Data  
Privacy: Legal and Ethical Issues  
Telephone Tap Detector*

*Foreign Intelligence Surveillance Court of Review  
Laser Listening Devices  
Privacy: Legal and Ethical Issues  
Telephone Recording Laws  
Telephone Recording System  
Telephone Scrambler*

## Telephone Tap Detector

A telephone tap detector aids communication security by providing electronic recognition of attempts to intercept a call through wiretapping or listening devices. Telephone tapping is, at least in certain particulars, an exact science, and tap detection technology must likewise be efficient to counteract those efforts. With telephone tapping no longer an extremely infrequent aspect of daily life, tap detectors have become a popular item among security-conscious consumers.

In tapping into a phone line, surveillance personnel use technology akin to that which an electrician might apply in attempting to siphon power from an electric line. However, whereas an electric wire attached to a circuit receives a regular supply of power, a telephone tap cannot maintain constant access to a telephone line, or it would be too easy to detect. Instead, the tap actually “seizes” the telephone line as a call is coming in.

The tap is most likely to engage between the first and third ring of an incoming call, and from that point onward, assuming all conditions are reasonably favorable for surveillance, the tap remains in effect for the duration of the call. A telephone tap detector recognizes this seizure of the phone line, and provides further verification once the call concludes. Depending on the number and timing of disconnection reactions after the receiver is reengaged, a good tap detector (consumer models sell for several hundred dollars) can determine whether wiretapping equipment is in the process of disengaging from the phone line.

### ■ FURTHER READING:

#### PERIODICALS:

Cloud, David S. and David Rogers. “Telecom Firms Lobby for Funding of Upgrades to Ease Surveillance.” *Wall Street Journal*. (April 5, 2000): A4.

“How Secure Are Your Phone, Fax, Data Transmission Systems?” *Security* 34, no. 6 (June 1997): 75–76.

Kupperschmid, David. “James Bond ‘Supplier’ Has the Cure for Whatever Is Bugging You.” *Los Angeles Times*. (April 26, 1985): 2.

“Texas Politicians’ Cases Prompt New Interest in Eavesdropping.” *San Francisco Chronicle*. (December 18, 1995): A12.

#### SEE ALSO

*Domestic Intelligence*

## Terror Alert System, United States

■ JOSEPH PATTERSON HYDER

On March 12, 2002, President Bush created the Homeland Security Advisory System (HSAS) by signing Homeland Security Presidential Directive 3. The HSAS is a five-tiered alert system designed to quickly notify government agencies, industry, and the public about terrorist threats to United States interests at home and abroad. The White House established the HSAS under the Attorney General’s office in conjunction with the Office of Homeland Security, but the Department of Homeland Security (DHS) now controls the HSAS. The goal of this color-coded alert system is to increase effective communication and cooperation among the various federal, state, and local agencies that would be involved in the event of a terrorist attack and to make the public more aware of the threat of a terrorist attack.

Before the establishment of the HSAS, numerous federal and local agencies utilized their own threat level assessments. These threat level assessments were used to notify specific agencies or sectors of government about possible attacks on American interests. The federal agencies that made such assessments did not readily disseminate this information to the American public or to state and local governments. Various agencies also acted on different intelligence reports, leading to disparate threat assessments. The HSAS provides a framework for these various alert systems.

One of the most publicized components of the HSAS is its color-coded warning system. This system consists of five Threat Conditions, each accompanied with suggested Protective Measures. The five Threat Conditions are Low (Green), Guarded (Blue), Elevated (Yellow), High (Orange), and Severe (Red). The DHS and Attorney General devised the HSAS to provide an easy way for local governments and the public to assess the current situation and take appropriate action.

The Department of Homeland Security has also devised a set of recommended actions, or Protective Measures, for local governments, industry, and the public to follow based on the alert level. These recommendations include increased security for public events, increased



# HOMELAND SECURITY ADVISORY SYSTEM

**SEVERE**

**SEVERE RISK OF  
TERRORIST ATTACKS**

**HIGH**

**HIGH RISK OF  
TERRORIST ATTACKS**

**ELEVATED**

**SIGNIFICANT RISK OF  
TERRORIST ATTACKS**

**GUARDED**

**GENERAL RISK OF  
TERRORIST ATTACKS**

**LOW**

**LOW RISK OF  
TERRORIST ATTACKS**

The five-level, color-coded terrorism warning system, enacted in 2002, is a response to public comments that broad terror alerts issued by the government raised alarm without providing useful guidance. AP/WIDE WORLD PHOTOS.

surveillance, and implementation of local emergency response plans.

The Department of Homeland Security defines the Low Condition (Green) as indicating a low risk of terrorist attacks. Under the Green level, government agencies and private industry should train personnel and analyze emergency plans. The Guarded Condition (Blue) indicates a general risk of terrorist attacks. Protective Measures dictate updating emergency procedures and keeping the public informed. The Elevated Condition (Yellow) signals a significant risk of terrorist attack. Under this condition, surveillance of sensitive locations is increased and emergency plans are readied and implemented, when necessary.

The Department of Homeland Security declares a High Condition (Orange) when specific and collaborated information indicates a significant risk of terrorist attack. Under an Orange alert, security is tightened at high-profile public events, and the events are cancelled, if necessary. Access may also be restricted to sensitive areas, such as dams, nuclear power facilities, and government buildings. A Severe Condition (Red) signifies a severe risk of terrorist activity. A Red alert is only declared when there is a real and significant threat. Emergency personnel are reassigned as needed, transportation is closely monitored or redirected, and public facilities may be closed.

Critics of the HSAS assert that the Threat Conditions system claim that the color-coded Threat Conditions may actually be detrimental to national security. These critics claim that the DHS holds the Threat Conditions at an artificially high level in order to give the appearance of preparedness and to avoid public outcry if a terrorist attack occurred at a low threat level. In addition, critics contend that leaving the color-coded warning at an artificially high level will erode public trust in the system.

The Department of Homeland Security counters its critics by maintaining that elevating the Threat Condition when warranted deters terrorism by showing that America is vigilant. Additionally, an elevated Threat Condition alerts law enforcement to increase its efforts to combat terrorism. The Department of Homeland Security also has set criteria for raising or lowering the Threat Condition. The DHS weighs the credibility, specificity, and gravity of every piece of intelligence that is interpreted as a potential threat. The DHS, in conjunction with the FBI, CIA, and other agencies, then seeks to corroborate specific threats. Based on their findings, the DHS will then raise or lower the Threat Condition either for the entire nation or for a specific region.

#### ■ FURTHER READING:

##### ELECTRONIC:

United States Department of Homeland Security. <<http://www.dhs.gov>> (May 2003).

##### SEE ALSO

*Homeland Security, United States Department*

## Terrorism, Domestic (United States)

■ JUDSON KNIGHT

The U.S. Federal Bureau of Investigation (FBI) defines domestic terrorism as terrorism involving groups based in, and operating entirely within, the United States and its territories, without foreign direction. The FBI further divides domestic terrorism into three basic categories: right-wing, left-wing, and special-interest terrorism. Terrorist organizations in the United States had their beginnings with the foundation of the Ku Klux Klan in 1866. White racist movements remain major contributors to terrorism, but the toll of terrorist activities has also included socialist, anarchist, and minority nationalist groups, as well as terrorism associated with the environment and animal rights. Of the 205 lives claimed in terrorist incidents within the United States between 1980 and 1999, more than 80% died in a single attack: the bombing of the Alfred P. Murrah Federal Building in Oklahoma City on April 19, 1995.

### Domestic Terrorist Groups

At the center of domestic counterterrorism efforts is the FBI, whose Counterterrorism Division defines domestic terrorism thus in a 1999 report titled *Terrorism in the United States*:

“Domestic terrorism involves groups or individuals who are based and operate entirely within the United States or its territories without foreign direction, and whose acts are directed at elements of the U.S. government or population. Domestic terrorist groups can represent right-wing, left-wing, or special interest orientations. Their causes generally spring from issues relating to American political and social concerns.”

**Right-wing terrorism.** Right-wing terrorist groups, as defined by the FBI, are motivated by notions of white racial supremacy, as well as anti-government and anti-regulatory beliefs. They may also include extremist Christian groups such as those that bomb abortion clinics, although these groups are sometimes lumped in with special-interest terrorists. Moreover, many acts of right-wing terrorism, such as racially motivated attacks by “skinhead” gangs, are legally classified as hate crimes rather than domestic terrorism. They thus fall within the realm of the FBI Criminal Division, rather than the Counterterrorism Division.

Not all anti-government groups are necessarily racist: for example, some members of the militia movement in the 1990s attempted to distance themselves from anti-black and anti-Semitic hate groups. On the other hand, all

these groups are united by a suspicion of, or hatred for, the federal government, often coupled with a conspiratorial view of history and politics. These putative conspiracies may have their origins in Washington—which, in the view of many right-wing terrorist groups, seeks to take away Americans' guns and impose ruinous taxes and regulations on them—or they may be international in origin. Many of these groups in the 1990s, for instance, spoke of black helicopters supposedly operated by United Nations forces on U.S. soil.

**The Ku Klux Klan.** Strictly speaking, the Ku Klux Klan is not a terrorist organization, as its acts of violence have tended to be retaliatory rather than symbolic. Still, given its influence on events in the United States, no discussion of right-wing terrorism would be complete without its mention

Formed by ex-Confederate soldiers after the Civil War, the Klan was an attempt to strike back at the federal government for its imposition of martial law and military occupation in the South. However, the victims of Klan violence—recently freed slaves—were far more vulnerable than the Southern whites, no matter how disenfranchised and dispossessed as they might have seen themselves to be. The Klan, which terrorized and killed African Americans throughout the South, was outlawed by the Ku Klux Klan Act of 1871. In 1882, the U.S. Supreme Court declared the Klan Act unconstitutional, but by then Reconstruction was over, and the Klan had faded into the background.

D. W. Griffith's 1915 film *Birth of a Nation* helped influence the formation of a new Ku Klux Klan at Stone Mountain, Georgia. Over the next decade, the Klan grew in strength nationwide, and prominent persons—including future U.S. Supreme Court Justice Hugo Black—belonged to the organization. Ironically, it was the Klan in 1925, before Martin Luther King, Jr., was born, who undertook the first major "March on Washington" of the twentieth century.

During the 1950s and 1960s, Klansmen conducted terrorist attacks and acts of murder against African Americans and civil rights workers, but the triumph of the civil rights movement spelled the end of the Klan as a force. In the 1970s and 1980s, the Southern Poverty Law Center and other anti-racist organizations successfully gutted the Klan with a series of lawsuits. With its assets stripped, the organization split into numerous splinter groups.

**Other racist groups.** Alongside Klan movements have been other racist groups, most notably the American Nazi Party (whose founder, George Lincoln Rockwell, was assassinated in 1967 by a member of his own party) and various "Aryan" organizations such as the White Aryan Brotherhood and the Aryan Nations. These groups have often found themselves confronted with a contradiction. Persons on the right, even the extreme right, tend to be

patriotic, if sometimes ambivalent about the government in power, whereas Nazi and Aryan groups ultimately pay homage to one of America's most hated historical enemies, Adolf Hitler.

On the other hand, many racist groups, such as the White Patriot Party, have built the "patriot" theme into their name. Others, such as the so-called "Christian Identity Movement" (whose members reject that name) identify white America with the 10 lost tribes of Israel. The Christian Identity Movement and other such groups are profoundly anti-Semitic. None of these groups is, in strict terms, a terrorist group (though they are certainly classifiable as hate groups), but as with the Klan, discussions of right-wing terrorism require reference to such groups.

The bible for adherents of white racist and anti-government belief systems is not Hitler's *Mein Kampf*, but a distinctly American version, more dime novel than political manifesto. This is *The Turner Diaries* by Andrew MacDonald, a.k.a. William Pierce. Published in 1978, the novel pictures a race war that results in the triumph of whites over blacks, Jews, and other "mongrels." It identifies April 20, 1999, as the 110th birthday of "The Great One" (Hitler was born April 20, 1889), and depicts a terrorist bombing of a government building that seems to have provided Oklahoma City bomber Timothy McVeigh with a model for his attack.

**Anti-government groups.** The remainder of right-wing terrorist groups are united by an anti-government stance that may or may not also embrace racism. Such groups emerged on the national scene with a February 13, 1983, attack on law enforcement officers in Medina, North Dakota, by a group named the Sheriff's Posse Comitatus.

The years since have seen a proliferation of groups such as the various "militias" (anti-government paramilitary groups organized at a state level) or the Freemen. Some of these engage in terrorism by other means, such as the filing of bogus liens and other groundless legal claims that tie up government resources. Sometimes referred to as "paper terrorism," these acts clogged up courts in some western states during the 1990s.

Just as the Klan had a natural base in the South, and some racist groups have found a home in the Midwest (for instance, the American Nazis, which operate primarily in Chicago), the wide-open spaces of the West have provided a natural venue for anti-government groups and individuals. Many of these reacted strongly to the 1992 FBI raid against the Ruby Ridge, Idaho, residence of white separatist Randy Weaver, which resulted in the death of Weaver's wife and son.

The presidency of William J. Clinton proved particularly odious to anti-government groups and individuals, who perceived the Clinton administration as leftist. Anti-government groups claimed that Attorney General Janet Reno was to blame for the April 19, 1993, attack on the Waco, Texas compound of the Branch Davidians, a religious sect reportedly hoarding a cache of illegal weapons.



After a 51-day siege by the Bureau of Alcohol, Tobacco, and Firearms, a combined FBI and Delta Force team assaulted the compound, whereupon the Branch Davidians set the buildings on fire. Seventy-six people, including cult leader David Koresh, died in the conflagration. Outside the compound, a group of anti-government protesters, which had been keeping vigil for weeks, watched as the blaze erupted. Among those present was a 25-year-old Persian Gulf War veteran named Timothy McVeigh.

**Oklahoma City.** Exactly two years after the Waco incident, at 9:02 a.m. on April 19, 1995, a Ryder rental truck parked in front of the Murrah Federal Building in Oklahoma City exploded. Inside the truck was a 4,800-pound bomb of ammonium nitrate and fuel oil, a combination similar to that used in the 1993 World Trade Center blast. The blast tore a hole along the side of the nine-story building, injuring some 500 persons and killing 168—including 19 infants in a day-care center.

Within minutes, word began to spread throughout the nation that—in a variation on language that would often be used by members of the media in the next few days—“terror had struck the heartland.” Authorities already had two suspects, who they had named “John Doe No. 1” and “John Doe No. 2,” and initially many reporters speculated that Muslim extremists had caused this blast, as they had the World Trade Center bombing. The men ultimately charged for the Oklahoma City bombing, however, would turn out to be from much closer to home.

About 90 minutes after the blast, police in Perry, Oklahoma, stopped McVeigh for driving without a license plate. When they searched his trunk, they discovered anti-government literature, along with significant traces of PETN, a compound used in the making of the bomb. Soon afterward, having recovered the vehicle identification number of the Ryder truck from its axle, authorities traced it to a rental outlet in Junction City, Kansas, where the owner identified McVeigh as the man who had rented the truck under the name “Robert Kling.” McVeigh also matched the composite sketch of “John Doe No. 1.”

On April 21, federal authorities arrested McVeigh, along with brothers Terry and James Nichols. James was later released, but McVeigh and Terry Nichols stood trial. Although McVeigh had been involved with the militia movement for a time, he had long since separated himself from any group. His philosophy was strongly anti-government, and it appears that he chose the Murrah Building because he thought (incorrectly) that the personnel involved at Waco worked in that building.

Both McVeigh and Nichols were found guilty, and McVeigh was given the death penalty, while Nichols received a life sentence without parole. McVeigh was executed on June 11, 2001. Exactly three months later, the foreign-sponsored terrorist attacks in New York City, Washington, and Pennsylvania, would eclipse the Oklahoma City death toll by a factor of nearly 20.

## Left-Wing and Special Interest Terrorists

So great has been the impact of right-wing terrorism, due to the Oklahoma City bombing (as well as the visibility of hate groups such as the Klan and neo-Nazis), that the significance of left-wing and special interest terrorism has tended to be obscured. In these cases, the death toll is much smaller, but a number of incidents have claimed lives and property.

Left-wing terrorists, according to the FBI, have a revolutionary socialist agenda, and present themselves as protectors of the populace against the alienating effects of capitalism and U.S. imperialism. Notable early participants in left-wing terrorism were various socialist and anarchist groups from the late nineteenth and early twentieth centuries. Leon Czolgoz, who shot President William McKinley in 1901, embraced anarchist beliefs, though no anarchist group would accept him for membership.

**Puerto Rican nationalists.** From the 1950s, Puerto Rican nationalists have been among the most prominent left-wing terrorists. These might seem at first glance to have a special-interest agenda, but due to their socialist rhetoric and goals, the FBI has categorized them as left-wing terrorists. On November 1, 1950, members of the Puerto Rican Nationalist Party attempted to assassinate President Harry S Truman, and during the 1950s, members of the group stormed the U.S. House of Representatives.

On May 1, 1961, Puerto Rican-born Antuilo Ramirez Ortiz hijacked a National Airlines flight and diverted it to Havana. This was the first successful hijacking of a U.S. plane, and Ortiz, who returned to the United States in 1975, was sentenced to 25 years for his crime. On January 27, 1975, members of the Armed Forces for Puerto Rican Liberation (known by its initials in Spanish, FALN), bombed a bar on Wall Street in New York City, killing four and wounding 60.

**The late 1960s and early 1970s.** Two days after the FALN attack, members of the Weather Underground claimed responsibility for a bombing at the U.S. State Department in Washington, D.C. The “Weathermen,” as they were commonly known (after a line from the song “Subterranean Homesick Blues” by Bob Dylan), were formed from the radical Students for a Democratic Society group in 1969. Their leaders received training in Havana, and over the next few years, they conducted a wave of bombings and robberies. Their death toll was small, however, and consisted primarily of three group members killed when a bomb they were building accidentally exploded at a Greenwich Village townhouse in March 1970.

The late 1960s and early 1970s was also the heyday of the Black Panther Party and other African American nationalist groups that used terrorist tactics. Among the

most notorious events associated with the Black Panthers was an August 7, 1970, raid on a California courthouse by University of California professor Angela Davis and Jonathan Jackson on behalf of Jackson's imprisoned brother George. Davis and Jackson kidnapped several people, critically wounded a district attorney, and killed a judge. Jackson died in the struggle, and on August 21, 1971, George Jackson died in a prison riot he incited after his lawyer reportedly smuggled a pistol to him.

Also notable among left-wing groups of the era was the Symbionese Liberation Army (SLA), which on February 5, 1974, kidnapped heiress Patricia Hearst. Formed in 1973, the group declared war on "fascism," which it equated with America, and it waged its war primarily through bank robberies. Hearst, allegedly brainwashed by the group, adopted the name "Tania" and participated in the robberies. Most of its members, including leader Donald DeFreeze, were killed in a May, 1974, shootout with authorities. Hearst was captured by the FBI in September, 1975. In January, 2001, outgoing president Clinton pardoned her, along with several Puerto Rican revolutionaries held in federal prisons.

**Rudolph and Kaczynski.** Special-interest terrorism, as its name indicates, is focused on specific issues. Such terrorism tends to be predominantly left-wing, but there are exceptions, most notably the acts attributed to Eric Robert Rudolph. These might be classified as right-wing attacks, as the bombing targets included abortion clinics and a nightclub frequented by homosexuals. On the other hand, the bombing at Atlanta's Centennial Olympic Park on July 27, 1996, during the 1996 Olympics, an attack that killed two people and injured 112, is not currently tied to an obvious political agenda. As of mid-2003, Rudolph had evaded capture, and remained on the FBI's "Ten Most Wanted" list.

Also difficult to classify are the crimes of Theodore Kaczynski, the accused Unabomber. Beginning in 1978, when a bomb disguised as a package went off at Northwestern University, a mysterious bomber terrorized universities and airlines (hence the name *una* in the nickname given to him by the FBI). After a total of 10 attacks on universities and airlines, the Unabomber struck a computer store in Sacramento, California, on December 11, 1985, causing his first fatality.

The Unabomber was spotted on February 20, 1987, placing a bomb at another computer store, this one in Salt Lake City, Utah. This sole sighting provided authorities with a sketch of the Unabomber, who then ceased activities for six years. In June 1993, after two more bombings that month, the Unabomber sent the *New York Times* a letter outlining an agenda based in environmental and anarchist themes. His last two attacks, in 1994 and 1995 (the latter just five days after Oklahoma City) struck an advertising executive and a timber industry lobbyist respectively, again suggesting an anti-capitalist, environmentalist agenda.

After reading the Unabomber's manifesto, David Kaczynski noted similarities between the writer and his brother Ted, and alerted authorities. Ted Kaczynski, once a promising mathematics graduate student, had abandoned society for the isolation of a cabin in Montana, where he was arrested on April 3, 1996. In January 1998, on the eve of his trial, a judge rejected Kaczynski's request to represent himself in court. Kaczynski filed a guilty plea, and was sentenced to life in prison. Though Kaczynski's acts seem terroristic, inasmuch as they are arguably directed at human beings as symbols rather than purely as humans, the FBI did not officially classify his bombings as domestic terrorism, noting a "lack of information regarding the subject's motivation."

**Special-interest terrorism in the 1990s.** In the 1990s, special-interest terrorism of the political right included attacks and threats against abortion clinics. Special-interest terrorism on the political left involved motivations that included the environment, animal rights, and opposition to globalization. The FBI paid special note to the left-wing groups in this instance, not because of political bias, but because attacks on abortion clinics are classified as hate crimes, giving them an entirely different legal definition and involving other arms of the national justice system.

On the other hand, the acts of groups such as the Animal Liberation Front (ALF) or the Earth Liberation Front (ELF) fit within the FBI's definition of terrorism. The ALF, affiliated with similar groups worldwide, conducts raids on research laboratories and other facilities where, in the view of group members, animals are mistreated. Radical environmentalists have been charged with "tree spiking," or putting metal spikes in trees to harm loggers who cut them, and of mailing packages rigged with razor blades. In October 1998, the ELF was charged with setting fire to a ski resort in Vail, Colorado.

The FBI also noted the rise of anti-globalization demonstrations, which are founded in an opposition to the growth and international influence of Western corporations and financial entities. Though officially grouped with left-wing terrorism because of its strongly anarchist undertones, anti-globalization activities might also be considered special-interest in nature. During the World Trade Organization ministerial meetings in Seattle from November 30 to December 3, 1999, anti-globalization demonstrators conducted extensive acts of vandalism.

## CONPLAN

On June 21, 1995, just two months after the Oklahoma City bombing, President Clinton issued Presidential Decision Directive (PDD) 39, "U.S. Policy on Counterterrorism." Its purpose was to provide guidelines for deterring terrorism on America's shores, as well as terrorism against Americans and allies abroad. In accordance with PDD 39 and PDD 62, issued the same day, U.S. government agencies developed the United States Government

Interagency Domestic Terrorism Concept of Operations Plan, or CONPLAN for short.

Presented in January 2001, CONPLAN outlines the response to a domestic terrorist attack, or a foreign-sponsored terrorist attack on U.S. soil, such as those that occurred eight months later, on September 11. CONPLAN identifies the FBI as the lead agency for domestic counterterrorism, and the Federal Emergency Management Agency (FEMA) as the lead consequence management agency. It also outlines responsibilities for the Attorney General and Department of Justice, FEMA, the Environmental Protection Agency, and the departments of Defense, Energy, and Health and Human Services.

## ■ FURTHER READING:

### BOOKS:

Abanes, Richard. *American Militias: Rebellion, Racism, and Religion*. Downers Grove, IL: InterVarsity Press, 1996.

Ellis, Richard J. *The Dark Side of the Left: Illiberal Egalitarianism in America*. Lawrence, KS: University Press of Kansas, 1998.

George, John, and Laird Wilcox. *American Extremists: Militias, Supremacists, Klansmen, Communists, and Others*. Amherst, NY: Prometheus Books, 1996.

*Terrorism in the United States 1999*. Washington, D.C.: Federal Bureau of Investigation, 1999.

### SEE ALSO

*Architecture and Structural Security*  
ATF (United States Bureau of Alcohol, Tobacco, and Firearms)

*Coordinator for Counterterrorism, United States Office*  
*Domestic Emergency Support Team, United States*  
*Domestic Intelligence*

*Domestic Preparedness Office (NDPO), United States*  
*National*

*FBI (United States Federal Bureau of Investigation)*

*GAO (General Accounting Office, United States)*

*General Services Administration, United States*  
*Terrorism, Intelligence Based Threat and Risk Assessments*  
*Terrorism, Philosophical and Ideological Origins*

*Terrorism Risk Insurance*

*Terrorist and Para-State Organizations*

*Terrorist Organizations, Freezing of Assets*

*Terrorist Threat Integration Center*

*United States, Counter-Terrorism Policy*

recommendations for United States municipalities. By May 1998, GAO reported, only 11 cities had put in place the necessary emergency response systems. Intelligence-based terrorism threat and risk assessments gained much greater import after the terrorist attacks of September 11, 2001, but the U.S. intelligence community often found itself in the challenging situation of recommending public warnings without inciting panic or alternately, complacency.

In 1996, Congress passed legislation whereby law enforcement and emergency response personnel in 120 of the largest cities nationwide were required to undertake training in order to become prepared for the possibility of a terrorist attack. To assist in these preparations, Washington appropriated \$30 million in training funds. Yet, according to an April 1998 GAO report, *Combating Terrorism: Threat and Risk Assessments Can Help Prioritize and Target Program Investments*, fewer than a dozen cities had undergone the necessary training. Figures provided by two House members showed that, in fact, 22 cities had completed this training, but in any case, only about one in six of America's major cities was prepared.

According to GAO's report, "While it is not possible to reduce risk to all potential targets against . . . terrorism, risk assessments can help ensure that training, equipment, and other safeguards are justified and implemented based on threat, the vulnerability of the asset to an attack, and the importance of the asset." The Department of Defense (DOD), placed in charged of the preparedness project, questioned the need for risk assessments, which DOD officials claimed would raise implementation costs by as much as \$30,000 per city. According to DOD representatives, risk assessments would not affect a city's choice of preparedness equipment.

In December 1998, four months after the Islamic terror network al-Qaeda bombed two U.S. embassies in Africa, U.S. intelligence learned of plans for another attack orchestrated by al Qaeda leader Osama bin Laden. The *New York Times* reported the advisory, but the end of the year passed without incident.

A year later, intelligence sources warned of an attack to occur on December 31, 1999, and although U.S. authorities apprehended suspected al-Qaeda operatives, the story gained little attention in the U.S. media. This time, Americans were more concerned about the apparent Year 2000 problem, or computer glitches associated with the transition from 1999 to 2000.

## Terrorism, Intelligence Based Threat and Risk Assessments

■ JUDSON KNIGHT

In the 1990s, a terrorism risk assessment conducted by the General Accounting Office (GAO) led to preparedness

## The Post-September 11, 2001, environment

In April 2002, the Bush administration received what it believed to be credible information concerning a planned suicide bombing on a major U.S. bank. Aside from the threat itself, the White House was faced with the challenge



Explosive materials and electric igniting devices are shown in the car of a suicide bomber just 300 yards from the U.S. Embassy in Kabul, Afghanistan, where he was stopped by a chance traffic accident in July 2002. AP/WIDE WORLD PHOTOS.

of determining how much to tell the American people so as to keep them properly informed but not spark mass hysteria—and not give away too much information concerning the intelligence resources used in making the threat assessment. Fortunately, the threat passed, but the issue of how to handle suspected threats has not been resolved. When the Office of Homeland Security suggested in February 2003 that Americans purchase duct tape and plastic sheeting to guard their homes against a possible chemical attack, the announcement was greeted with more derision than panic.

The idea of risk assessments dates back to the early Cold War, when intelligence agencies on both sides of the iron curtain were concerned with sizing up one another's relative nuclear and conventional weapons and capabilities. With the end of the Cold War and the rise of international terrorist groups as America's principal foe, risk and threat assessment has become much more challenging. Some experts in the field use the term "net assessment," referring to a complex of factors that includes both the actual threats and the perception of those threats. Integral

to such risk assessments, then, is some quantifiable determination of the psychological state both of the terrorists and the threatened population.

#### ■ FURTHER READING:

##### BOOKS:

- Cameron, Gavin. *Nuclear Terrorism: A Threat Assessment for the 21st Century*. New York: St. Martin's Press, 1999.
- Cordesman, Anthony H. *Terrorism, Asymmetric Warfare, and Weapons of Mass Destruction: Defending the U.S. Homeland*. Westport, CT: Praeger, 2002.
- Haugen, David M. *Biological and Chemical Weapons*. San Diego: Greenhaven Press, 2001.
- Roukis, George S., and Hugh Conway. *Global Corporate Intelligence: Opportunities, Technologies, and Threats in the 1990s*. New York: Quorum Books, 1990.

##### PERIODICALS:

- Burns, Jimmy. "Assessing Terror Threat Raises Whitehall Tension." *Financial Times*. (December 14, 2002): 5.

Cummings, Jeanne, and Gary Fields. "Calculating Risks: For Two Tense Days, Bush Team Wrestled with Vague Threat." *Wall Street Journal*. (May 17, 2002): A1.

#### ELECTRONIC:

Summary/Review of Reports Concerning Threats by Osama Bin Laden. Cornell University Library. <<http://www.library.cornell.edu/colldev/mideast/bladen98.htm>> (April 7, 2003).

#### SEE ALSO

*HUMINT (Human Intelligence)*  
*Kenya, Bombing of United States Embassy*  
*Terrorism Risk Insurance*  
*Terrorist Threat Integration Center*  
*Vulnerability Assessments*

## Terrorism, Philosophical and Ideological Origins

■ ERIC v.d. LUFT

Terrorism is the systematic belief in the political, religious, or ideological efficacy of producing fear by attacking—or threatening to attack—unsuspecting or defenseless populations, usually civilians, and usually by surprise. Terrorist attacks are desperate acts of those who feel themselves to be otherwise powerless. Terrorism is self-righteous, absolutist, and exclusivist. In general, terrorist policy adherents are unwilling or unable to negotiate with their perceived enemies, or prevented by political, social, or economic circumstances from doing so. The philosophical underpinnings of terrorism have become well established worldwide.

The terms "terrorism" and "terrorist" came into the language in the 1790s when British journalists, politicians, orators, and historians used them to describe the Jacobins and other particularly violent French revolutionaries. The terms have evolved since then, and now typically refer to furtive acts by unknown, underground perpetrators, not overt acts by people in power. Nevertheless, some terrorists are secretly harbored, underwritten, trained, or commanded by states that have vested interests against the terrorists' targets. Examples of state-sponsored terrorism include Afghanistan's support of al-Qaeda in 2001, Libya's involvement in the destruction of Pan Am Flight 103 over Lockerbie, Scotland, in 1988, and Adolf Hitler (1889–1945) ordering the Reichstag burned down in 1933 so that he could blame the Communists.

Terrorism as we now understand it was not possible until the invention of gunpowder and subsequent explosives and incendiaries. Before that, small cadres of insignificant conspirators generally lacked the means to achieve sudden massive destruction by stealth. Gunpowder enabled weaklings to outmatch and regularly defeat strong

warriors for the first time in history. In a historical sense, modern terrorism began with the unrealized November 5, 1605 "Gunpowder Plot" of Guy Fawkes (1570–1606), who, had he lived in the twelfth century, could not have threatened king and parliament as he did in the seventeenth. But even with the ever-widening proliferation and availability of explosives since then, acts of terrorism remained rare until the middle of the nineteenth century, when anarchism arose as an ideological force.

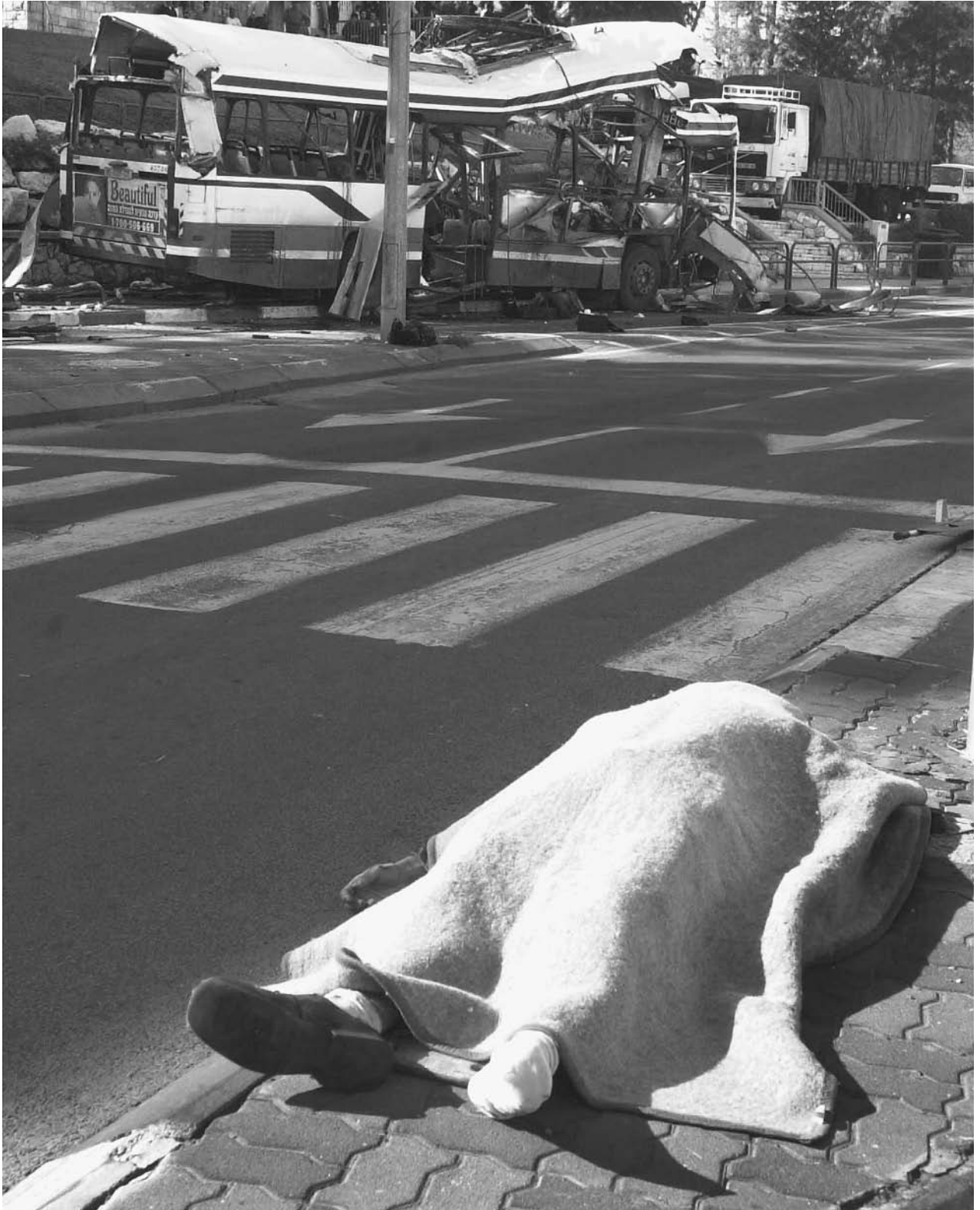
The systematic theory of modern political terrorism arose in Germany during the *Vormā*, i.e., the time between the accession of Prussian King Friedrich Wilhelm IV (1795–1861) in 1840 and the revolutions of 1848. Edgar Bauer (1820–1886) and Mikhail Bakunin (1814–1876), two of the three principal anarchists in the "Young Hegelians," were among terrorism's earliest ideological proponents. The Young Hegelians were a loosely organized group of radical intellectuals influenced to various degrees by the dialectical logic of Georg Wilhelm Friedrich Hegel (1771–1830), the dominant German philosopher of the first half of the nineteenth century. Hegel could not have foreseen that his thought would be perverted in this way and would not have approved of terrorism in any form.

Almost every ideology that became important in the twentieth century arose from the Young Hegelians. These second-generation disciples of Hegel ramified his allegedly self-unifying thought into many disparate movements: socialism and communism came from Karl Marx (1818–1883) and Friedrich Engels (1820–1895), socialism and Zionism from Moses Hess (1812–1875), secular humanism from Ludwig Feuerbach (1804–1872), the "higher criticism" of sacred texts from David Friedrich Strauss (1808–1874) and Bruno Bauer (1809–1882), dialectical historicism from August von Cieszkowski (1814–1894), political liberalism from Arnold Ruge (1802–1880), existentialism and anthropological materialism from Karl Schmidt (1819–1864), individualistic anarchism from Max Stirner (1806–1856), utopian anarchism from Bakunin, and raw anarchism and political terrorism from Edgar Bauer.

In chronological order of their earliest terrorist writings, the first six major theorists of terrorism were Edgar Bauer, Bakunin, Wilhelm Weitling (1808–1871), Karl Heinzen (1809–1880), Sergei Nechaev (1847–1882), and Johann Most (1846–1906).

Edgar Bauer became involved with radical groups in 1839 while a student at the University of Berlin. By 1842 both he and his close friend Engels were members of "The Free Ones" (*Die Freien*), the most notorious club of intellectual agitators in Germany in the early 1840s. His first book, *Bruno Bauer and his Enemies* (1842), defended his brother against government persecution, urged violence, and threatened the Prussian regime with a return to the French Revolution. His 1843 polemic, *Critique's Struggle with Church and State*, advocated terrorism even more blatantly and earned him a prison sentence.

Bakunin, a Russian noble by birth, studied Hegelianism in Russia from 1836 to 1840 and in Berlin from 1841 to



The body of a victim lays covered on the ground at the scene of a bus bomb, background, after a Palestinian suicide bomber detonated nail-studded explosives on the bus in the northern Israeli port city of Haifa in December 2001. AP/WIDE WORLD PHOTOS.

1842. In October 1842, under the pseudonym Jules Elysard, he published "Reaction in Germany," a revolutionary article in Ruge's *Deutsche Jahrbücher*. This essay recommended insurgent violence with lines such as: "The urge to destroy is also a creative urge." Bakunin soon distanced himself from Young Hegelianism, but retained his mutinous attitude toward church and state. His extreme anarchism and nihilism were best expressed in *God and the State*, written in 1871 but published posthumously in 1882.

Weitling was a German tailor who became politically active in 1843. He wrote letters, broadsides, tracts, pamphlets, and books inciting the proletariat to all sorts of violent crimes to free themselves from their oppressors. Even firebrands among the communist, socialist, anarchist, or syndicalist movements who advocated guerrilla tactics to achieve their political goals were appalled by Weitling's 1843 suggestion that revolutionaries could use arson, theft, and murder to their advantage.

Heinzen is sometimes regarded as the ideological father of modern terrorism, despite the prior writings of Edgar Bauer, Bakunin, and Weitling. Heinzen wrote in 1848 and published in 1849 a powerful essay, "Murder," which claimed that not only the assassinations of leaders, but even the mass murders of innocent civilians, could be effective political tools and should be used without regret. He fled Germany in 1849 and immigrated to America as a "48er," a refugee from the 1848 revolutions. He edited German-language newspapers, notably *Der Pionier*, in several American cities. Although he never specifically recanted his terrorist beliefs, he became a relatively peaceful socialist. He and his wife lived the last twenty years of his life in Roxbury, Massachusetts, as tenants and friends of a prominent early woman physician, Marie Zakrzewska (1829–1902), one of *Der Pionier's* most ardent supporters.

Nechaev, the son of a former Russian serf, learned early to hate government in general and the czarist regime in particular. As a student at the University of St. Petersburg in 1868, his radical agitations soon forced him into exile. He met Bakunin in Geneva, Switzerland, in March 1869, and became briefly his disciple. They co-wrote several inflammatory pamphlets, including *The Revolutionist's Catechism* (1869), an unrestrained exhortation to anti-government violence, urging relentless cruelty toward all enemies of the revolution and absolute devotion to the cause of destroying the civilized world. Nechaev returned to Russia in August 1869, murdered a political rival named Ivanov in December 1869, and fled back to Geneva. The Swiss extradited him to Russia in 1872. Convicted of murder in 1873 and sentenced to twenty years of hard labor in Siberia, he died in prison under mysterious circumstances. Fedor Dostoevskii (1821–1881) based his character Pyotr Verkhovensky in *The Possessed* (1871) on Nechaev.

Most was a Social Democrat member of the Reichstag who was forced to flee Germany during Otto von Bismarck's (1815–1898) "Red Scare" of 1878. In exile Most became more radical, relinquished Marxism for anarchism,

and edited an inflammatory newspaper, *Die Freiheit*, first in London, briefly in Switzerland, and after 1882 in America. Embittered after serving eighteen months of hard labor in a British prison and after the German Social Democrat Party expelled him *in absentia*, his motto became "Long live hate!" He fell in love with dynamite and spent the rest of his career praising it, learning how to use it, and teaching his fellow revolutionaries how to steal it and the money needed to buy it. He probably invented the letter-bomb, though there is no evidence that he ever used one himself. American agents arrested him for sedition in 1901 because *Die Freiheit* quoted Heinzen's line, "Murder the murderers," the same day that anarchist Leon Czolgosz (1873–1901) killed President William McKinley (1843–1901).

## ■ FURTHER READING:

### BOOKS:

- Breckman, Warren. *Marx, the Young Hegelians, and the Origins of Radical Social Theory: Dethroning the Self*. Cambridge: Cambridge University Press, 1999.
- Browning, Gary K. *Hegel and the History of Political Philosophy*. London: Macmillan; New York: St. Martin's, 1999.
- Calvert, Peter. "Terror in the Theory of Revolution," *Terrorism, Ideology, and Revolution*, edited by Noel O'Sullivan. Boulder, Colo.: Westview, 1986.
- Confronting Fear: A History of Terrorism*, edited by Isaac Cronin. New York: Thunder's Mouth, 2002.
- Laqueur, Walter. *A History of Terrorism*. New Brunswick, N.J.: Transaction, 2002.
- Luft, Eric v.d. "Edgar Bauer and the Origins of the Theory of Terrorism," *The Left-Hegelians: New Philosophical and Political Perspectives*, edited by Douglas Moggach and Andrew Chitty. Albany: SUNY Press, forthcoming.
- Mah, Harold. *The End of Philosophy, the Origin of "Ideology": Karl Marx and the Crisis of the Young Hegelians*. Berkeley: University of California Press, 1987.
- Marx, Karl, and Friedrich Engels. *The German Ideology*, translated by S. Ryazanskaya. Moscow: Progress, 1964.
- . *The Holy Family, or, Critique of Critical Critique*, translated by R. Dixon. Moscow: Foreign Languages Publishing House, 1956.
- Nomad, Max. *Apostles of Revolution*. Boston: Little, Brown, 1939.
- Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind*, edited by Walter Reich. Baltimore: Johns Hopkins University Press, 1998.
- Stirner, Max. *The Ego and His Own*, translated by Steven Byington, revised and edited by David Leopold. Cambridge: Cambridge University Press, 1995.
- The Terrorism Reader*, edited by David Whittaker. London: Routledge, 2001.
- Wittke, Carl Frederick. *The Utopian Communist: A Biography of Wilhelm Weitling, Nineteenth-Century Reformer*. Baton Rouge: Louisiana State University Press, 1950.

### SEE ALSO

*Terrorism, Intelligence Based Threat and Risk Assessments*

*Terrorist and Para-State Organizations  
Terrorist Organization List, United States*

## Terrorism Risk Insurance

■ JUDSON KNIGHT

On November 26, 2002, President George W. Bush signed into law the Terrorism Risk Insurance Act. Intended to cover the private sector in the event of terrorist attacks such as those that occurred on September 11 of the preceding year, the Act provided a system of shared public and private compensation for insured losses resulting from acts of terrorism. The insurance industry was divided in its response to the new legislation, and the high cost of coverage kept away many potential policyholders in the nation's major cities.

On signing the Act, Bush, surrounded by construction workers, announced that "Today we're taking action to strengthen America's economy, to build confidence with America's investors, and to create jobs for America's workers." In recent months, he said, a lack of terrorism insurance had resulted in the delay or cancellation of more than \$15 billion in real estate sales.

The new legislation would speed economic recovery in the event of a terrorist attack by providing insurance against such incidents. Not only had such coverage been far from explicitly delineated in many traditional policies, but if a single insurer had to compensate even a fraction of the losses result from an event such as September 11, it could bankrupt the company.

The new law would put in place a temporary federal program to establish such insurance, and rescinded all exclusions to terrorism coverage in existing policy. By backing the new insurance with federal funds, it would also afford the insurance industry an opportunity to stabilize in the new market conditions created by the terrorist attacks. After taking effect on the day it was signed, the law would expire automatically in three years.

The insurance industry was divided in its response, a situation captured by headlines that appeared in two different industry journals over the space of a little more than a week: "TRIA Already Is a Success" (*Business Insurance*, February 24, 2003) and "One-Size-Fits-All TRIA Doesn't Fit" (*National Underwriter*, March 3). The first article, despite its positive spin on the new program, noted that "risk manager response hasn't exactly been overwhelming." One of the problems, noted an industry expert quoted in the second article, was that the law excluded domestic terrorism. Given the sometimes fine line between foreign and domestic terrorists, this could prove problematic.

A report in the *New York Times* that appeared the same day as the *National Underwriter* story noted that

corporations in New York City, Washington, D.C., Chicago, and other large cities—areas where terrorist attacks in the future were most likely—had shown little interest in purchasing the new insurance. The reasons were several, including the high cost of premiums, combined with the fact that the federal government would compensate most of the losses in the event of a major terrorist attack.

The article also cited the lack of coverage for an attack by domestic terrorists, a flaw given the fact that prior to September 2001, the worst terrorist attack in American history was perpetrated by Americans—in Oklahoma City on April 19, 1995.

### ■ FURTHER READING:

#### PERIODICALS:

Bumiller, Elisabeth. "Government to Cover Most Costs of Insurance Losses in Terrorism." *New York Times* (November 27, 2002): A1.

Bush, George W. "Remarks on Signing the Terrorism Risk Insurance Act of 2002." *Weekly Compilation of Presidential Documents* 38, no. 48 (December 2, 2002): 2096–97.

Hays, Daniel. "One-Size-Fits-All Doesn't Fit: Study." *National Underwriter* 107, no. 9 (March 3, 2003): 26.

Romano, Jay. "Terrorism Insurance, at a Price." *New York Times* (March 9, 2003): 5.

Treaster, Joseph B. "Insurance for Terrorism Still a Rarity." *New York Times* (March 8, 2003): C1.

"TRIA Already Is a Success." *Business Insurance* 37, no. 8 (February 24, 2003): 8.

#### ELECTRONIC:

Terrorism Risk Insurance Program. U.S. Department of the Treasury. <<http://www.ustreas.gov/offices/domestic-finance/financial-institution/terrorism-insurance/>> (March 28, 2003).

#### SEE ALSO

*September 11 Terrorist Attacks on the United States Terrorism, Intelligence Based Threat and Risk Assessments Treasury Department, United States*

## Terrorist and Para-State Organizations

Para-state organizations challenge some aspect of the authority of recognized governments or states. Many para-state groups, illegal within their own country or territory, seek international recognition at the Unrepresented Nations and Peoples Organization (UNPO), a non-governmental organization headquartered in The Hague.





Members of the Laskar Mujahidin listen to a briefing from their leader in Solo, Central Java, Indonesia, in October 2002, the same year that Washington branded the Islamist extremist group a terrorist organization. AP/WIDE WORLD PHOTOS.

There are no clear defining lines between guerilla forces and para-state organizations. Guerilla warfare refers to more organized, widespread, or formal armed resistance by paramilitary or para-state groups (usually wearing some sort of insignia or uniform) toward an occupying force. In many areas of the world, guerilla warfare tactics are used by paramilitary groups against government forces.

Moreover, history is replete with causes and movements, initially branded as “illegitimate” or “para-state” organizations that ultimately become the ruling government (i.e., transforming the group from a “para-state” to the state itself). In some cases, an organization branded “terrorist” or “outlaw” by the ruling government may be considered a legitimate political movement or a group of “fighters” for a cause embraced by a segment of the population.

For example, the African National Congress—once headed by Nobel Laureate Nelson Mandela—was for decades branded a terrorist and outlaw group by the now abolished apartheid South African government.

In general, it is the commission of acts of violence that brand organizations as para-state terrorist groups as opposed to legitimate political parties or national liberation movements that do not engage in violence or armed struggle in an attempt to change governments.

The definition of terrorist is, however, not entirely subjective. Under United States law, terrorist activity is so labeled by “any activity which is unlawful under the laws of the place where it is committed (or which, if committed in the United States, would be unlawful under the laws of the United States or any State) and which involves any of the following: The hijacking or sabotage of any conveyance (including an aircraft, vessel, or vehicle); The seizing or detaining, and threatening to kill, injure, or continue to detain, another individual in order to compel a third person (including a governmental organization) to do or abstain from doing any act as an explicit or implicit condition for the release of the individual seized or detained; A violent attack upon an internationally protected person (defined in section 1116(b)(4) of title 18, United States Code) or upon the liberty of such a person; or an assassination.”

# MGA KIDNAPPER! MGA MAMAMATAY-TAO!



Abu Sabaya



Hamsiraji Sali



Khadafi Janjalani



Abu Solaiman



Isnilon Hapilon

## PREMYO PARA SA IMPORMASYON HANGGAN \$5,000,000

The U.S. Government is offering a reward of up to \$5,000,000 for information leading to the arrest or conviction of the terrorists responsible for the kidnapping of Martin and Gracia Burnham, and the kidnapping and murder of Guillermo Sobero. If you have any information about any individuals committing acts of international terrorism against U.S. persons or property, please contact the U.S. Embassy.

PREMYO PARA SA KATARUNGAN

[www.rewardsforjustice.net](http://www.rewardsforjustice.net)

1-800-10-739-2737 (MANILA) 1-800-877-3927 (USA)

Kung Cell phone ang gagamitin ay tumawag lamang sa 02-526-9832/9833/9834

LAHAT NG IMPORMASYON NA MATATANGAP NAMIN AY ITUTURING SIKRETO



A handout circulated by the U.S. embassy in Manila after announcing the U.S. government's offer of a \$5 million reward in May 2000, for the capture of leaders of the Abu Sayyaf Islamist extremist group that kidnaped two Americans and killed another on Basilan Island, southern Philippines. AP/WIDE WORLD PHOTOS.

U.S. law and statutes also define as acts of terrorism “the use of any biological agent, chemical agent, or nuclear weapon or device; or explosive, firearm, or other weapon or dangerous device. . . with intent to endanger, directly or indirectly, the safety of one or more individuals or to cause substantial damage to property.”

**State-sponsored terrorism.** In addition to para-state organizations that usually operate within defined borders, a state itself can also act to sponsor terrorism or terrorist organizations.

As of April 1, 2003, the U.S. State Department had designated the following countries state sponsors of international terrorism: Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria. The State Department asserts that although “. . . most no longer engage directly in terrorist activity, they may support terrorist groups by providing funding or arms.”

**Terrorist organizations.** Annually, the U.S. Department of State publishes a list of designated foreign terrorist organizations (FTOs). In 2002, the State Department designated 33 groups as FTOs. The State Department’s formal list focuses on groups who have recently engaged in terrorist attacks or are otherwise highly active. In addition, the State Department’s annual report to Congress, *Patterns of Global Terrorism*, also identifies and profiles organizations that in the past have been designated as terrorist organizations.

Organizations not formally designated as foreign terrorist groups, but listed as terrorist organizations in the 2001 report to Congress include the following organizations: Alex Boncayao Brigade (ABB); Al-Ittihad al-Islami (AIAI); Allied Democratic Forces (ADF); Anti-Imperialist Territorial Nuclei (NTA); Army for the Liberation of Rwanda (ALIR); Cambodian Freedom Fighters (CFF); Continuity Irish Republican Army (CIRA); First of October Antifascist Resistance Group (GRAPO); Harakat ul-Jihad-I-Islami (HUJI); Harakat ul-Jihad-I-Islami/Bangladesh (HUJI-B); Islamic Army of Aden (IAA); Irish Republican Army (IRA); Al Jama’a al-Islamiyyah al-Muqatilah bi-Libya; Japanese Red Army (JRA); Jemaah Islamiya (JI); Kumpulan Mujahidin Malaysia (KMM); Lord’s Resistance Army (LRA); Loyalist Volunteer Force (LVF); New People’s Army (NPA); Orange Volunteers (OV); People Against Gangersterism and Drugs (PAGAD); Red Hand Defenders (RHD); Revolutionary Proletarian Initiative Nuclei (NIPR); Revolutionary United Front (RUF); The Tunisian Combatant Group (TCG); Tupac Amaru Revolutionary Movement (MRTA); Turkish Hizballah; and the Ulster Defense Association/Ulster Freedom Fighters (UDA/UVF).

#### ■ FURTHER READING:

##### ELECTRONIC:

CDI (Center for Defense Information), Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <<http://www.cdi.org/terrorism/terrorist.cfm>> (April 17, 2003).

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. “Patterns of Global Terrorism 2001,” Annual Report: On the record briefing. May 21, 2002 <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

#### SEE ALSO

*Terrorism, Philosophical and Ideological Origins*  
*Terrorist Organization List, United States*  
*Terrorist Organizations, Freezing of Assets*

---

## Terrorist Organization List, United States

---

The United States Secretary of State formally designates “Foreign Terrorist Organizations” (FTO) that threaten United States interests. Within the Department of State, the Office of the Coordinator for Counterterrorism is assigned the primary responsibility for monitoring available intelligence and public news accounts of terrorist activities so that they may advise the Secretary on decisions related to terrorism-related designations. The designation process, in part, focuses on groups who have recently engaged in terrorist attacks.

Although designations can be modified at any time (i.e., groups can be added or deleted from the list by the Secretary of State) designations normally expire in two years unless renewed. Changes in the list require a formal notification of Congress. Organizations have the right under U.S. law—should they choose to appear—of appealing an FTO designation to United States Court of Appeals for the District of Columbia Circuit within 30 days of such designation.

**Impact of FTO designation.** When an organization is designated as an FTO it becomes unlawful for a person in the United States (or U.S. jurisdictions) to knowingly provide “material support or resources” (e.g. money, aid, advice, training, etc.) to a designated FTO.

FTO members may not legally enter the U.S. or its territories, and may be deported upon discovery.

U.S. banks or other financial institutions that control accounts in which agents of FTOs have some interest must report account existence and activities to the Office

of Foreign Assets Control of the U.S. Department of the Treasury.

**Designated FTOs.** The U.S. Department of State publishes a list of designated foreign terrorist organizations as a part of its report, *Patterns of Global Terrorism*, submitted annually to Congress.

Groups designated as foreign terrorist organizations by the U.S. Department of State, as of January 30, 2003, include the following organizations: "Abu Nidal Organization (ANO); Abu Sayyaf Group; Al-Aqsa Martyrs Brigade; Armed Islamic Group (GIA); Asbat al-Ansar; Aum Shinrikyo; Basque Fatherland and Liberty (ETA); Communist Party of the Philippines/New People's Army (CPP/NPA); Gama'a al-Islamiyya (Islamic Group); HAMAS (Islamic Resistance Movement); Harakat ul-Mujahidin (HUM); Hizballah (Party of God); Islamic Movement of Uzbekistan (IMU); Jaish-e-Mohammed (JEM) (Army of Mohammed); Jemaah Islamiya organization (JI) al-Jihad (Egyptian Islamic Jihad); Kahane Chai (Kach); Kurdistan Workers' Party (PKK); Lashkar-e Tayyiba (LT) (Army of the Righteous); Liberation Tigers of Tamil Eelam (LTTE); Mujahedin-e Khalq Organization (MEK); National Liberation Army (ELN); Palestine Liberation Front (PLF); Palestinian Islamic Jihad (PIJ); PFLP-General Command (PFLP-GC); Popular Front for the Liberation of Palestine (PFLP); al-Qaeda; Real IRA; Revolutionary Armed Forces of Colombia (FARC); Revolutionary Nuclei (formerly ELA); Revolutionary Organization 17 November; Revolutionary People's Liberation Army/Front (DHKP/C); Salafist Group for Call and Combat (GSPC); Shining Path (Sendero Luminoso, SL); United Self-Defense Forces of Colombia (AUC)."

#### ■ FURTHER READING:

##### ELECTRONIC:

CDI (Center for Defense Information), Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <<http://www.cdi.org/terrorism/terrorist.cfm>> (April 17, 2003).

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001, Annual Report: On the Record Briefing." May 21, 2002 <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual Reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

##### SEE ALSO

*Guerilla Warfare*  
*Terrorism, Philosophical and Ideological Origins*  
*Terrorist and Para-State Organizations*  
*Terrorist Organizations, Freezing of Assets*

## Terrorist Organizations, Freezing of Assets

■ MARTIN J. MANNING

Monitoring the frozen assets of terrorist organizations is something that took on a new focus and urgency after the events of September 11, 2001. The United States and its allies have arrested about 2,290 suspected terrorists and terrorist financiers in 99 countries, designated about 250 individuals and organizations as terrorists or terrorist supporters, and seized more than \$113 million in assets since the terrorist attacks of September 11, 2001.

On September 24, 2001, President George W. Bush stated, "We will direct every resource at our command to win the war against terrorists, every means of diplomacy, every tool of intelligence, every instrument of law enforcement, every financial influence. We will starve the terrorists of funding." The president directed the federal government to wage the nation's war against the financing of global terrorism, and we have continued to devote our resources and extensive expertise to fulfill this mandate. In actions and in words, the Treasury Department has shown that in the war against terrorism, financial intermediaries and facilitators who infuse terrorist organizations with money, materiel, and support will be held accountable along with those who perpetrate terrorist acts.

Immediately after the terrorist attacks, Congress worked closely with the Department of the Treasury, along with the Department of Justice and other agencies and departments, to make significant improvements in the law that enhances Treasury's ability to tackle the issue of terrorist financing in a more unified, cohesive and aggressive manner. Of particular importance to the counter-terrorist efforts, the U.S. Patriot Act, enacted into law on October 26, 2001, expanded the law enforcement and intelligence community's ability to access and share critical financial information regarding terrorist investigations. In the months immediately following the September 11 attacks, the Department of the Treasury took six principal steps to identify and pursue financial underwriters of terrorism:

- worked with other U.S. Government agencies to implement Executive Order 13224;
- established Operation Green Quest, an inter-agency task force, to target financial networks and mechanisms;
- won the adoption of UN Security Council Resolutions 1373 and 1390 which require member nations to disrupt terrorist financing;
- engaged other multilateral institutions such as the Financial Action Task Force (FATF) and the international financial institutions to focus on terrorist financing;



New People's Army guerrillas, the armed wing of the Communist Party of the Philippines (CPP), photographed at a clandestine assembly in the Cordillera region in northern Philippines, 2002. ©AFP/CORBIS.

- implemented the U.S. Patriot Act provisions to broaden and deepen access to critical financial information in the war against terrorist financing and to expand the anti-money laundering regulatory network;
- shared information across the federal government, with the private sector and among U.S. allies to crack down on terrorist financiers.

For the first time, the 2002 National Money Laundering Strategy (NMLS) contained such a strategy, with a discrete set of objectives and priorities targeting terrorist financing. Goal Two of the NMLS identified financial mechanisms or systems by which terrorist funding was initiated and sought to attack these mechanisms on an interagency and coordinated basis. The NMLS stated that terrorist groups tap into a wide range of sources for their financial support, including otherwise legitimate enterprises, such as construction companies, honey shops, tanneries, banks, agricultural commodities growers and brokers, trade businesses, bakeries, restaurants, and bookstores. The strategy focused on the following areas:

- targeted intelligence gathering;
- freezing of suspect assets;
- law enforcement actions;

- diplomatic efforts and outreach;
- smarter regulatory scrutiny;
- outreach to the financial sector; and
- capacity building for other governments and the financial sector through Treasury and other departmental technical assistance programs.

The NMLS is an integrated inter-agency strategy that draws on the expertise and resources of the Treasury Department, the Department of Justice, the Department of State and other departments and agencies of the federal government, as well as on foreign partners and on the private sector. Its mission is to first, identify appropriate financial targets through technology, intelligence, investigative resources, and regulations to locate and freeze the assets of terrorists, wherever they may be located.

Second, the NMLS freezes terrorist-related assets on a global scale. The U.S. government has frozen over U.S. \$35 million in terrorist-related assets since September 11, 2001, and the international community has frozen an additional U.S. \$78 million. More important than the dollars frozen is the dismantling of these financial pipelines, which served to transmit far greater sums of money for terrorist purposes. Third, the NMLS coordinates effective

law enforcement actions, both domestically and internationally, against terrorist cells and networks. Internationally, Treasury has deployed Customs attachés and representatives from Treasury's Office of Foreign Assets Control (OFAC) in strategic embassies around the world to facilitate cooperation with host countries and regions in combating terrorist financing. Between September 12, 2001, and October 28, 2002, international law enforcement cooperation has led to approximately 2290 arrests of suspected terrorists and their financiers in 99 countries.

Fourth, together with other agencies, the NMLS uses existing diplomatic resources and regional and multi-lateral engagements to ensure international cooperation, collaboration and capability in dismantling terrorist financing networks. One of the bilateral initiatives is the U.S. Government's designation of Foreign Terrorist Organizations (FTOs). Under authorities provided by the Antiterrorism and Effective Death Penalty Act of 1996, the Secretary of State, in consultation with the Attorney General and the Secretary of the Treasury, has designated 35 groups as foreign terrorist organizations. The designations make it a criminal offense for American persons to knowingly provide funds or other forms of material support for these designated groups. Some other countries have used the designations as a guideline for their own efforts to curb terrorism financing.

Fifth, the NMLS implements smarter regulatory scrutiny by training the financial sectors to concentrate enhanced due diligence and suspicious activity monitoring on terrorist financing and money laundering typologies. Through the U.S. Patriot Act authorities, Treasury has been able to expand regulatory scrutiny to all businesses within the financial sector that may be susceptible to terrorist or criminal abuse. Sixth, the NMLS regulates expansion under the authorities of the Patriot Act in full consultation with the private financial sectors.

On October 1, 2002, FinCEN's (Financial Crimes Enforcement Network) secure link with financial institutions, the Patriot Act Communications System (PACS), became operational along with several capacity-building initiatives with other governments and the private sector with respect to terrorist financing. For example, Treasury is co-chairing a FATF Working Group on Terrorist Financing, which, among other issues, is charged with identifying technical assistance needs of various governments around the world. This Working Group is collaborating with donor states, the International Monetary Fund, the World Bank, and the UN Counter-Terrorism Committee in coordinating the delivery of technical assistance to those governments.

## Actions Taken Against Terrorist Financing

The most visible and immediately effective tactic of U.S. terrorist financing strategy has been designating and blocking the accounts of terrorists and those associated with

financing terrorist activity. Publicly designating terrorists, terrorist supporters and facilitators, and blocking their ability to receive and move funds through the world's financial system has been and is a crucial component in the fight against terrorism. On September 24, 2001, President Bush issued Executive Order 13244, "Blocking Property and Prohibiting Transactions with Persons Who Commit, Threaten to Commit, or Support Terrorism."

The Department of the Treasury's Office of Enforcement, in conjunction with Treasury's Office of International Affairs and the Office of Foreign Assets Control, has helped lead U.S. efforts to identify and block the assets of terrorist-related individuals and entities within the United States and worldwide. Currently, 250 individuals and entities are publicly designated as terrorists or terrorist supporters by the United States, and since September 11th, over \$113 million in assets of terrorists has been frozen around the world. Beyond simply freezing assets, these U.S. and international actions to publicly identify terrorists and their supporters advance global interests in terrorist financing and combating terrorism by:

- shutting down the pipeline by which designated parties moved money and operated financially in the mainstream financial sectors;
- informing third parties who may be unwittingly financing terrorist activity of their association with supporters of terrorism;
- providing leverage over those parties not designated who might otherwise be willing to finance terrorist activity;
- exposing terrorist financing "money trails" that may generate leads to previously unknown terrorist cells and financiers;
- forcing terrorists to use alternative and potentially more costly informal means of financing their activities; and
- supporting diplomatic effort to strengthen other countries' capacities to combat terrorist financing through the adoption and implementation of legislation that allows states to comply with their obligations under UN Security Council Resolutions 1390 and 1373.

Currently, over 165 countries and jurisdictions have blocking orders in force. Alternative financial mechanisms to combat terrorist financing conducted through these mechanisms include the following measures.

**Protecting charities from terrorist abuse.** Under the authority of E.O. [Executive Order] 13224, the United States has designated twelve charitable organizations as having ties to al-Qaeda or other terrorist groups. In addition, the United States has designated and blocked the assets of the largest U.S.-based Islamic charity, which acted as a funding vehicle for the HAMAS terrorist organization.

The FATF Special Recommendation VIII on Terrorist Financing commits all member nations to ensure that non-profit organizations cannot be misused by financiers of

terrorism. The United States is co-chairing the FATF Terrorist Financing Working Group that has recently produced an international best practices paper on how to protect charities from abuse or infiltration by terrorists and their supporters.

Efforts are underway to assist U.S.-based charities concerned that their distribution of funds abroad might reach terrorist-related entities and trigger a blocking action on the part of the Treasury Department—the Department has developed voluntary best practices guidelines for all U.S.-based charities. The Treasury Department developed these guidelines in response to requests from the Arab American and American Muslim communities, who reported a reduction in charitable giving and an increased apprehension among donors as a consequence of the Treasury Department’s blocking of the three domestic charities.

**Regulating *Hawalas*: informal value transfer systems.** Terrorists have also used *Hawalas* and other informal value transfer systems as a means of terrorist financing. The word “hawala” (meaning “trust”) refers to a fast and cost-effective method for the worldwide remittance of money or value, particularly for persons who may be outside the reach of the traditional financial sector. In some nations, *Hawalas* are illegal; in others they are active but unregulated. It is, therefore, difficult to measure accurately the total volume of financial activity associated with the system; however, it is estimated that, at a minimum, tens of billions of dollars flow through *Hawalas* and other informal value transfer systems on an annual basis.

The United States has already taken steps to regulate *Hawalas* and informal value transfer systems. The U.S. Patriot Act requires money remitters (informal or otherwise) to register as “money services business” or “MSBs,” thereby subjecting them to existing money laundering and terrorist financing regulations, including the requirement to file Suspicious Activity Reports (SARs). As a result, well over 11,000 money service businesses have registered with the federal government and are now required to report suspicious activities. The Act makes it a crime for the money transfer business owner to move funds that he knows are the proceeds of a crime or are intended to be used in unlawful activity. Failure by money service business principals to register with FinCEN and/or failure to obtain a state license also are federal crimes.

FATF Special Recommendation VI addresses this issue by demanding that countries register or license informal value transfer businesses and subject them to all of the FATF Recommendations that applies to banks and non-bank financial institutions. In addition, at a conference on hawala in the United Arab Emirates (UAE) in May, 2002, a number of governments agreed to adopt FATF Special Recommendation VI and shortly thereafter, the UAE government announced it would impose a licensing requirement on hawala operators operating within its borders. Participants at the UAE meeting drafted and

agreed upon the Abu Dhabi Declaration on Hawala, which set forth a number of principles calling for the regulation of *Hawalas*.

**Combating bulk cash smuggling.** Bulk cash smuggling has proven to be yet another means of financing adopted by terrorists and their financiers. Customs has executed 650 bulk cash seizures totaling \$21 million, including \$12.9 million with a Middle East connection. Pursuing bulk cash smuggling from a domestic perspective, however, is not enough; disruption of this tactic requires a global approach.

**Investigating trade-based terrorist financing.** With respect to trade-based financial systems, authorized enforcement agencies continue to investigate the use of licit and illicit international trade commodities, for example, diamonds, gold, honey, and cigarettes, as well as narcotics, to fund terrorism. The U.S. Customs Service has developed a state-of-the-art database system to identify anomalous trade patterns for imports and exports to and from the United States. In the past, Customs has demonstrated this system to other nations, including Colombia, with excellent results.

**Investigating terrorist cyber-fundraising activities.** Terrorist groups now exploit the Internet to recruit supporters and raise terrorist funds. Developing a strategy to counter such cyber-fundraising activities is a responsibility that the Treasury Department assumed in its 2002 Anti-Money Laundering Strategy.

**Operation “Green Quest.”** On October 25, 2001, Treasury created Operation Green Quest (OGQ) to focus the Treasury Department’s financial expertise in the war against terrorist financing. OGQ identifies and attacks terrorist financing through a systemic financial approach. OGQ specializes in identifying financial mechanisms, such as illegal money remitters, and searching those systems to identify potential terrorist financing.

OGQ is led by the United States Customs Service, and includes the Internal Revenue Service, the Secret Service, the Bureau of Alcohol Tobacco and Firearms (ATF), Treasury’s Office of Foreign Assets Control (OFAC), FinCEN, the Postal Inspection Service, the Federal Bureau of Investigation (FBI), and the Department of Justice. The financial expertise of the Treasury Bureaus, along with the exceptional experience of our partner agencies and departments, is also utilized in this operational attack on terrorist financing.

## International Efforts

Internationally, the United States has worked not only through the United Nations on blocking efforts, but also through multi-lateral organizations and on a bi-lateral

basis to promote international standards and protocols for combating terrorist financing. The Treasury Department has continuously engaged the international community in developing and strengthening counter-terrorist financing initiatives and regimes.

The United Nations 1267 Committee is responsible for UN designations of individuals and entities associated with al Qaeda, Osama bin Laden, and the Taliban. States wishing to propose a name for UN designation typically include a statement of the basis for designation, along with identifying information for the use of financial institutions, customs and immigration officials, and others who must implement sanctions. If no state objects to the proposed designation within 48 hours after a name is circulated by the Committee Chairman, the designation becomes effective. The 1267 Committee then puts out an announcement on its web site and all UN member states are required to freeze any assets held by the designated party(ies), without delays.

**Financial Action Task Force (FATF).** Since 1989, the 31-member FATF has served as the preeminent anti-money laundering multilateral organization in the world. The United States has played a leading role in the development of this organization. Capitalizing on this financial crime expertise, on October 31, 2001, at the United States' initiative, the FATF issued Eight Special Recommendations on terrorist financing, requiring all member nations to:

- Ratify the UN International Convention for the Suppression of the Financing of Terrorism and implement relevant UN Resolutions against terrorist financing;
- Criminalize the financing of terrorism, terrorist acts and terrorist organizations;
- Freeze and confiscate terrorist assets;
- Require financial institutions to report suspicious transactions linked to terrorism;
- Provide the widest possible assistance to other countries' laws enforcement and regulatory authorities for terrorist financing investigations;
- Impose anti-money laundering requirements on alternative remittance systems;
- Require financial institutions to include accurate and meaningful originator information in money transfers; and
- Ensure that non-profit organizations cannot be misused to finance terrorism.

Many non-FATF countries have committed to complying with the Eight Recommendations and over 90 non-FATF members have already submitted self-assessment questionnaires to FATF describing their compliance with these recommendations. Together with the Departments of State and Justice, Treasury will continue to work with the FATF to build on its successful record in persuading

jurisdictions to adopt anti-money laundering and anti-terrorist financing regimes to strengthen global protection against terrorist finance.

As part of this effort, FATF has established a Working Group on Terrorist Financing (Working Group), which the United States is co-chairing with Spain, devoted specifically to developing and strengthening FATF's efforts in this field. At the most recent FATF Plenary in October, 2002, the Working Group, in collaboration with the World Bank, the International Monetary Fund, and the UN, identified a number of countries to receive priority technical assistance in order for them to come into compliance with the Eight Special Recommendations on Terrorist Financing.

**Egmont Group.** The Egmont Group represents 69 Financial Intelligence Units (FIUs) from various countries around the world. FinCEN is the FIU for the United States. The FIU in each nation receives financial information (such as SARs) from financial institutions pursuant to each government's particular anti-money laundering laws, analyzes and processes these disclosures, and disseminates the information domestically to appropriate government authorities and internationally to other FIUs in support of national and international law enforcement operations.

**Successful results.** International law enforcement cooperation has resulted in approximately 2290 arrests of suspected terrorists and their financiers in 99 countries from September 12, 2001 through October 28, 2002. Some of these arrests have led to the prevention of terrorist attacks in Singapore, Morocco and Germany, and have uncovered al-Qaeda cells and support networks in Italy, Germany, Spain, the Philippines and Malaysia, among other places. In addition, soon after September 11th, a Caribbean ally provided critical financial information through its FIU to FinCEN that allowed the revelation of a financial network that supported terrorist groups and stretched around the world.

On September 24, 2001, President Bush implemented Executive Order 13224 which expands the U.S. government's power and authority to target terrorist organizations to freeze and block their assets. In that same period, the United Nations adopted UN Security Council resolutions 1373 and 1390, directing member states to criminalize terrorist financing and adopt regulatory regimes to detect and deter terrorist financing. On August 29, 2002, the Office of Foreign Assets Control established the Specially Designated Nationals (SDN) and Blocked Persons List, which is updated as groups and individuals are added or removed. Most recently, in March 2003, the U.S. Department of the Treasury created a new unit to set strategy and policy for combating terrorist financing. The new Executive Office for Terrorist Financing and Financial Crimes would work with the financial services industry to locate terror-related accounts and groups. It will also oversee Treasury's Financial Crimes Enforcement Network



(FINCen), an investigative and information-gathering bureau, and the Office of Foreign Asset Controls (OFAC), which carries out U.S. orders blocking bank accounts and freezing assets of suspected terrorist groups and their supporters.

In order to continue Treasury's leadership on these critical issues, the new Office is charged with developing and implementing U.S. government strategies to combat terrorist financing domestically and internationally (in concert with Treasury's International Affairs Task Force on Terrorist Financing); developing and implementing the National Money Laundering Strategy, as well as other policies and programs to fight financial crimes; participating in the department's development and implementation of U.S. government policies and regulations in support of the Patriot Act, including outreach to the private sector; joining in representation of the United States at focused international bodies dedicated to fighting terrorist financing and financial crimes; and developing U.S. government policies relating to financial crimes.

#### ■ FURTHER READING:

##### BOOKS:

Blunden, Bob. *The Money Launderers: How They Do It, and How to Catch Them at It*. Chalford, England: Management Books, 2001.

Doyle, Charles. *The USA PATRIOT Act: A Legal Analysis*. Washington, D.C.: Congressional Research Service, Library of Congress, 2002.

Lilley, Peter. *Dirty Dealing: The Untold Truth about Global Money Laundering*. London: Kogan Page, 2000.

Naylor, R. T. *Wages of Crime: Black Markets, Illegal Finance, and the Underworld Economy*. Ithaca, NY: Cornell University, 2002.

Savla, Sandeep. *Money Laundering and Financial Intermediaries*. The Hague and Boston: Kluwer Law International, 2001.

U.S. Congress. House Committee on Financial Services. "Dismantling the Financial Infrastructure of Global Terrorism." Hearing, 107th Congress, 1st Session, Washington, D.C.: Government Printing Office, 2001.

———. House Committee on Financial Services. Subcommittee on Oversight and Investigations. "PATRIOT Act Oversight: Investigating Patterns of Terrorist Financing." Hearing, 107 Congress, 2nd session, February 12, 2002. Washington, D.C.: Government Printing Office, 2002.

U.S. Department of the Treasury. Financial Crimes Enforcement Network. "U.S. Compendium of Selected Anti-Money Laundering Statutes and Rules." Vienna, VA: 1997.

##### PERIODICALS:

Morais, Herbert V. "The War against Money Laundering, Terrorism, and the Financing of Terrorism," *Lawasia Journal* (2002): 1–32.

Serino, Robert B. "Money Laundering, Terrorism, and Fraud." *ABA Bank Compliance* (March/April 2002): 23–26.

Shams, Heba. "Using Money Laundering Control to Fight Corruption: An Extraterritorial Instrument." *International Financial and Economic Law* no. 27, 2000).

##### ELECTRONIC:

International Monetary Fund. "Enhancing Contributions to Combating Money Laundering: Policy Paper." <<http://www.imf.org/external/np/ml/2001/eng/042601.htm>> (April; 14, 2003).

International Monetary Fund. Financial System Abuse, Financial Crime and Money Laundering: Background Paper. <<http://www.imf.org/external/np/ml/2001/eng/021201.htm>> (April 14, 2003).

U.S. Treasury Department. "High Intensity Money Laundering and Related Financial Crimes Areas (HIFCAs) Designations" <[www.ustreas.gov/fincen/hifcadesignations.html](http://www.ustreas.gov/fincen/hifcadesignations.html)> (April 14, 2003).

U.S. Treasury Department, Office of Foreign Assets Control. "Specially Designated Nationals and Blocked Persons." <<http://www.ustreas.gov/offices/enforcement/ofac/sdn/t11sdn.pdf>> (April 14, 2003).

##### SEE ALSO

*IMF (International Monetary Fund)*  
*Intelligence and International Law*  
*Intelligence and Law Enforcement Agencies*  
*Intelligence Authorization Acts, United States Congress*  
*Intelligence Community*  
*Intelligence Officer*  
*Intelligence Policy and Review (OIPR), United States Office*  
*Intelligence Support, United States Office*  
*Secret Service, United States*  
*Terror Alert System, United States*  
*Terrorism, Intelligence Based Threat and Risk Assessments*  
*Terrorism, Philosophical and Ideological Origins*  
*Terrorist and Para-State Organizations*  
*Terrorist Organization List, United States*  
*Terrorist Threat Integration Center*  
*United States, Intelligence and Security*

## Terrorist Threat Integration Center

#### ■ CARYN E. NEUMANN

The Terrorist Threat Integration Center (TTIC) improves the ability of the United States to thwart terrorist attacks by analyzing and sharing intelligence emanating from anywhere in the world. Opened in May 2003, as part of President George W. Bush's initiative to revamp counterterrorism intelligence, the goal of the TTIC is to provide a comprehensive threat picture. While it operates under the direction of the Central Intelligence Agency chief, TTIC is staffed by counterterrorism experts from the CIA, Federal Bureau of Investigation (FBI) and the Departments of Defense and Homeland Security. It will eventually serve as the hub of all counterterrorism analysis.

In the wake of the 2001 World Trade Center attack, the intelligence gathering agencies in the United States came under heavy criticism from Congress and the public for their failure to predict and halt the terrorist assault. Government inquiries concluded that a lack of information sharing prevented anyone from doing sufficient analysis and taking action. The FBI, as the preeminent domestic intelligence agency, received the bulk of the blame. In response to these intelligence shortcomings, Bush established the TTIC and thereby ended the FBI's decades-long reign as the nation's chief provider of domestic intelligence.

The aim of the TTIC is to seamlessly unite intelligence from a variety of sources to assist executive branch policymaking decisions. To this end, TTIC has unfettered access to all terrorist threat intelligence from raw reports to finished analytic assessments. The analysts in the center measure the reliability of information from interrogated al-Qaeda prisoners, study warnings from foreign law-enforcement and spy agencies, assess tips from informants, examine satellite photos, and read transcripts of wiretapped conversations. No TTIC staff members conduct intelligence collection operations.

TTIC plays the lead role in creating a national counterterrorism structure to share across agency lines all terrorist threat intelligence, whether gathered in the U.S. or overseas. The tasking system of TTIC will be implemented in three phases. In its initial phase, the TTIC provides integrated terrorist threat analysis for the senior national leadership. The center's duties will include compiling the "daily threat matrix" that is instrumental to the president's decisions in the war on terror. In its secondary phase, TTIC will be the principal gateway for policymaker requests for analysis of potential terrorist threats to U.S. interests and will maintain a database of known and suspected terrorists that can be accessed by government officials at all levels who possess the appropriate security clearance. In its tertiary and final stage, TTIC will serve as the U.S. government hub for all terrorist threat-related analytic work.

As the TTIC is a joint venture of participating agencies, the Director of Central Intelligence, as statutory head of the U.S. intelligence community, oversees its activities. The head of the TTIC is selected by CIA chief in consultation with the Director of the FBI, the Attorney General, and the Secretaries of Homeland Security and Defense. At the initial stage, total staffing of TTIC is 60 U.S. government employees plus additional contractors. In the second phase of implementation, employment will rise to 120 people. In the final stage, TTIC will have a staff level of 250 to 300 employees. TTIC is scheduled to be located in a facility with the FBI Counterterrorism Division and the CIA Counterterrorist Center. This co-location is expected to enhance information sharing and maximize counterterrorism resources while reducing redundant capabilities.

The terrorist attack of September 11, 2001 made apparent the need to change the intelligence gathering strategy of the United States. While most government leaders and members of the public have applauded the goal of fusing intelligence analysis from the FBI and CIA, data

reflecting the efficiency of the TTIC to close intelligence gaps while safeguarding individual liberties will take months or years to accumulate.

#### ■ FURTHER READING:

##### ELECTRONIC:

United States Department of State, International Information Programs. "Fact Sheet: New Terrorist Integration Center Will Open May 1. February 14, 2003 <<http://usinfo.state.gov/topical/pol/terror/03021404.htm>> (February 25, 2002).

##### SEE ALSO

*Bush Administration (2001–), United States National Security Policy*  
*CIA (United States Central Intelligence Agency)*  
*United States, Counter-Terrorism Policy*  
*DCI (Director of the Central Intelligence Agency)*  
*DoD (United States Department of Defense)*  
*FBI (United States Federal Bureau of Investigation)*  
*Homeland Security, United States Department*  
*World Trade Center, 2001 Terrorist Attack*

## Thermal Body Scanners.

SEE *Communicable Diseases, Isolation, and Quarantine.*

## Thin Layer Chromatography

■ BRIAN HOYLE

Thin layer chromatography, which is typically abbreviated as TLC, is a type of liquid chromatography that can separate chemical compounds of differing structure based on the rate at which they move through a support under defined conditions.

TLC is useful in detecting chemicals of security concern, including chemical weapons, explosives, stabilizing chemicals for rocket propellants, and illicit drugs. For example, the Forensic Service Center of Lawrence Livermore National Laboratory has designed a computerized and portable TLC machine that can be taken to the field, and which has the ability to analyze 20 samples at a time. Analysis can be completed within 30 minutes.

TLC as it is still practiced today was introduced by Justus Kirchner in 1951. From its beginning, the technique was an inexpensive, reliable, fast, and easy to perform means of distinguishing different compounds from each other. The method was qualitative—it showed the presence of a compound but not how much of the compound

was present. In the late 1960s, TLC was refined so that it could reliably measure the amounts of compounds. In other words, the technique became quantitative. Further refinement reduced the thickness of the support material and increased the amount of the separating material that could be packed into the support. In High Performance TLC (HPTLC) the resolution of chemically similar compounds is better than with conventional TLC, and less sample is required. HPTLC requires specialized analysis equipment, and so is still not as popular or widespread as conventional TLC.

In TLC a solution of the sample is added to a layer of support material (i.e., grains of silica or alumina) that has been spread out and dried on a sheet of material such as glass. The support is known as the plate. The sample is added as a spot at one end of the plate. The plate is then put into a sealed chamber that contains a shallow pool of chemicals (the solvent), which is just enough to wet the bottom of the plate. As the solvent moves up through the plate support layer by capillary action, the sample is dragged along. The different chemical constituents of the sample do not move at the same speed, however, and will become physically separated from one another. The positions of the various sample constituents and their chemical identities are determined by physical methods (i.e., ultraviolet light) or by the addition of other chemical sprays that react with the sample constituents.

#### ■ FURTHER READING:

##### BOOKS:

Fried, Bernard, and Joseph Sherma. *Thin-Layer Chromatography (Chromatographic Science, V. 81)* New York: Marcel Dekker, 1999.

##### ELECTRONIC:

Lawrence Livermore National Laboratory. "Solid-Phase Microextraction." Forensic Science Center. May 6, 2002. <[http://www-ems.llnl.gov/s-t/solid\\_phase.html](http://www-ems.llnl.gov/s-t/solid_phase.html)>(March 5, 2003).

##### SEE ALSO

*Chemical and Biological Detection Technologies*  
Lawrence Livermore National Laboratory (LLNL)  
*Toxicology*

---

## TIA (Terrorism Information Awareness)

---

The Terrorism Information Awareness (TIA) system (formerly the Total Information Awareness program) is a new

intelligence database system that culls and stores information, and creates risk assessments for a variety of security and intelligence uses. Using communications and financial surveillance, as well as general intelligence information, the TIA system is able to sort information, identify patterns, and create data models. System developers predicted its use in security operations ranging from predicting terrorist attacks, to pre-flight screening of airline employees and passengers. The new program, developed by the Defense Advanced Research Projects Agency and managed by the Department of Homeland Security as part of the sweeping post-September 11 security reform, is controversial.

Critics fear that TIA facilitates the government's ability to create dossiers on average citizens. The Department of Defense pressed for the inclusion of medical, financial, and email records in the database. The collection of such personal information without cause or due process, raised questions about the system's implications on 4th Amendment search and seizure provisions.

TIA advocates, including U.S. Attorney General John Ashcroft, claim the system will promote a more thorough and rapid assessment of data, aiding international anti-terrorism measures. Opponents of the program assert that the database stores personal information, such as credit reports and organizational affiliations, violating privacy. Many also doubt that use of the TIA system will be limited to terrorist detection, infrastructure protection or other similar measures.

The debate over TIA (then known as the Total Information Awareness program) reached the Senate floor in January 2003, where legislators voted 100–0 to block immediate implementation of the system. The Senate barred the use of the system unless mandated by Congress after a thorough review of its implications for constitutional rights and legal entitlements to privacy.

Upon further deliberation in February, Congress and the Senate negotiated a deal in which TIA could possibly be used outside the United States by military and civilian intelligence forces, specifically for the identification of terrorist threats and the prevention of terrorism. The Wyden Amendment, named after the sponsoring Oregon senator, prohibited the domestic use of TIA technology and created a formal oversight process to review the impact of TIA operations. The Department of Defense was directed to provide a full assessment of the possible implications of TIA technology, or halt the program completely.

Although research continues on TIA functions, the future of the TIA program is pending as of May 2003. The Department of Defense, FBI, CIA, and Office of Homeland Security continue to advocate further development, and ultimately implementation, of TIA systems.

##### SEE ALSO

*APIS (Advance Passenger Information System)*  
*DOD (United States Department of Defense)*  
*Homeland Security, United States Department*

## Tissue-Based Biosensors

The military recognizes that biological cells are excellent sensors of changes in the environment because they respond to external stimuli with highly reproducible and specific signals. Some toxins cause cells to release oxygen radicals or nitrogen products. Other toxins result in the production of biochemical markers, such as enzymes or growth factors. Toxins may also induce structural or morphologic changes in cells. When cells are embedded in three-dimensional tissue constructs, they not only signal the presence of biological or chemical agents, but can also further indicate physiological consequences of exposure to these analytes.

The Defense Advance Research Projects Agency (DARPA) has initiated the Tissue-Based Biosensors Project, which provides funding to research and private institutions to develop two- and three-dimensional tissue-based biosensors that will accurately and efficiently determine the presence of biological and chemical weapons. The project specifically seeks to develop cell-based systems that can identify human health risks in the battlefield, improve the performance of cells for detection of chemical and biological weapons, enhance and extend the life of cells used as biosensors and impede the degradation of cellular biosensors when in operational use.

A variety of cell types can be used as biosensors, however, because of their inherent electrochemical nature, a majority of the research in the project focuses on developing neural cells and tissues as biosensors. One group, however, is studying physiological changes in bacteria known as extremophiles, because of their ability to withstand harsh environmental conditions. The systems that result from the research may take the form of three-dimensional scaffolds that harbor and nourish detector cells or flow through systems that identify signal cells. Some of the issues that researchers will address while working on this project include nutrient requirements for cells, transport mechanisms for nutrients and wastes, spatial requirements for cells within a three-dimensional matrix, cell signal detection and stability of tissue-based systems. New materials for culturing and maintaining cells in three-dimensional scaffolds will likely be developed.

### ■ FURTHER READING:

#### ELECTRONIC:

Defense Advanced Research Projects Agency. "Tissue-Based Biosensors" <<http://www.darpa.mil/dso/thrust/biosci/Tbb/index.html>> (March 3, 2003).

#### SEE ALSO

*Biodetectors*

*Bio-Engineered Tissue Constructs*  
*Biological and Biomimetic Systems*  
*Biological Input/Output Systems (BIOS)*  
*Biosensor Technologies*  
 DARPA (Defense Advanced Research Projects Agency)

## Tokyo Rose

■ ADRIENNE WILMOTH LERNER

During the Second World War, both Allied and Axis nations engaged in a multi-media propaganda battle. Leaflets, posters, film reels, and radio broadcasts were all used to spread misinformation and undermine the morale of enemy troops. Japanese Radio Tokyo broadcast an English language, anti-Allied program entitled the "Zero Hour." The program featured popular music and propagandist war reports read by women with alluring voices. While Radio Tokyo employed over 20 women on the program, the voices became collectively known among Allied soldiers as Tokyo Rose.

Though the moniker Tokyo Rose was popular legend, after the war, details of the Japanese Radio Tokyo propaganda program emerged that brought legend to life. An investigation revealed that Allied prisoners of war, under orders of their captors, produced "Zero Hour." The women who voiced the programs were mostly Japanese citizens. One of the women, however, was an American citizen. This changed the nature of the military investigations from a general inquiry to a treason case.

Iva Ikoku Toguri was born in California in 1916, a first-generation American citizen of Japanese descent. She attended the University of California, Los Angeles, and graduated in 1941. Shortly after graduation, Toguri went to Japan at her mother's request to care for a sick relative. Leaving in haste, she neglected to obtain an official passport that would aid her return to the United States. While in Japan, the Japanese military launched an attack on the American Pacific fleet at Pearl Harbor, bringing America into the Second World War. After war was declared on Japan, Toguri was denied her request to return to the United States. She refused to renounce her American citizenship, and was often placed under surveillance by the Japanese government as a possible enemy operative. Toguri spoke very little Japanese and from 1941 to 1943, she went to school to learn the language. She later took a job as a typist for Radio Tokyo in 1943. Because she knew English, Japanese executives at Radio Tokyo recruited her to voice the "Zero Hour" program. Toguri broadcast under the name Orphan Ann, and worked on the show until the end of the war.

Several war correspondents sought to find and interview the illusive, legendary, Tokyo Rose after the war. A



Iva Toguri D'Aquino, also known as Tokyo Rose, on her way to court in San Francisco, California in 1949, where she was on trial for treason and broadcasting propaganda to Allied troops during World War II. AP/WIDE WORLD PHOTOS.

colleague led reporters to Toguri, after accepting money offered by reporters for the interview. Assuming she had committed no crime as the broadcasts were directed and produced by prisoners of war, Toguri spoke freely with journalists about her role on Radio Tokyo. Conflicting reports exist about her reception of the nickname Tokyo Rose. The press about Toguri, along with the detailed notes of a couple of reporters, was brought to the attention of U.S. Army counter-intelligence.

United States Army authorities arrested Toguri in 1945. In 1948, she was brought to the United States and transferred to officers of the Federal Bureau of Investigation. After a five-year inquiry, Toguri was tried as the infamous Tokyo Rose on eight counts of treason. Acquitted of seven counts of treason, she was found guilty on the remaining charge of "speaking about the location and destruction of ships." She was sentenced to ten years in prison and a steep monetary fine. When released in 1956, she immediately sought to clear her name. She applied twice for a presidential pardon, but was denied.

The matter of Tokyo Rose disappeared from the public eye until a journalist in the 1970s probed for further information on the case. A series of articles revealed several incongruencies in the inquiry and trial of Toguri. Prosecutors argued that Toguri fled the United States

before the war and was possibly a Japanese intelligence agent, but scant evidence was offered. Testimonies of several Allied service members regarding the radio broadcasts were revisited, and Japanese records regarding the Radio Tokyo psychological warfare campaign were unearthed. Interviews of some of Toguri's wartime colleagues corroborated her earlier claims that she sometimes smuggled supplies and food for the Allied prisoners also employed on the "Zero Hour" program. Further interviews and documents revealed that information regarding ships and troop positions that Radio Tokyo broadcast was available in wartime America on short-wave radio and was selected by the POWs forced to work on the program because it was not immediately sensitive to the Allied war effort. The controversial treason case was never reopened by courts, but Toguri was issued a pardon by President Gerald Ford, in one of his last presidential acts, in 1977.

#### ■ FURTHER READING:

##### BOOKS:

Duus, Masayo, and Edwin O. Reischauer. Peter Duus (trans.) *Tokyo Rose: Orphan of the Pacific* Tokyo: Kodansha International, 1979.

##### SEE ALSO

*Propaganda, Uses and Psychology World War II*

## Tournament of Shadows.

SEE *Great Game*.

## Toxicology

#### ■ JUDYTH SASSOON

The science of toxicology is concerned with the adverse effects of chemicals on biological systems and includes the study of the detection, action and counteractions of poisons. Toxicologists today generally use the techniques of analytical chemistry to detect and identify foreign chemicals in the body, with a particular emphasis on toxic or hazardous substances. Toxins can be simple metal ions or more complex, inorganic and organic chemicals, as well as compounds derived from bacteria or fungi and animal-produced substances such as venoms. Poisons can range in their effects from a low-level debilitation to almost immediate death. Many drugs used to counter diseases can also be poisons at higher concentrations.

One of the most significant historical figures in the development of the science of toxicology was the Swiss physician and alchemist Paracelsus (1493–1541). He realized that there was a need for proper experimentation in the field of chemical therapeutics and distinguished between the therapeutic and toxic properties of substances, recognizing that they are indistinguishable except by dose. Paracelsus realized that it is not possible to categorize chemicals as either safe or toxic and laid the foundations for a key principle in toxicology known as the dose-response relationship. There is a graded dose-response relationship in individuals and a quantal dose-response relationship in a population. The quantal “all or none” dose-response is used to determine the median lethal dose (LD<sub>50</sub>), which estimates what percentage of the population would be affected by a dose increase. Estimation of LD<sub>50</sub> involves the use of at least two different animal species and doses of the chemical under test are administered by at least two different routes. Initially most of the test animals die within 14 days. Subacute exposure is then tested for a period of 90 days and long-term exposure testing takes a further 6 months to 2 years. Mathematical extrapolation is used to generalize results from animal testing to human risk incidence.

Another significant figure in toxicology was Spanish physician Orfila (1787–1853) who contributed to the specialty known as forensic toxicology. He devised methods of detecting poisonous substances and therefore provided the means of proving when criminal poisoning had taken place. After Orfila, toxicology developed further to include the study of mechanisms of poison action.

Forensic toxicology involves the use of toxicological methods for legal purposes. There is a considerable overlap between forensic and clinical toxicology, criminology, forensic psychology, drug testing, environmental toxicology, pathology, pharmacology, sports medicine and veterinary toxicology. The work of a forensic toxicologist generally falls into three main categories: identification of drugs such as heroin, cocaine, cannabis; detection of drugs and poisons in body fluids, tissues and organs; and measuring of alcohol in blood or urine samples. Results of the laboratory procedures must then be interpreted and presented to the legal courts.

A forensic toxicologist is normally given preserved samples of body fluids, stomach contents, and organ parts along with a coroner’s report containing information on symptoms and postmortem data. Specimens are generally divided into acidic and basic fractions for drug extraction from tissue or fluid. As an example, most of the barbiturate drugs are acid-soluble while most of the amphetamine drugs are base-soluble. After preliminary acid-base procedures, tissue or fluid samples are subjected to further laboratory tests consisting of screening tests and confirmation testing. Screening tests allow the processing of many specimens for a wide range of toxins in a short time and any positive indications from the screens are then verified with a confirmation test.

Laboratory methods used in toxicological analysis are various. Screening tests include (1) physical tests: testing the boiling point, melting point, density, and refractive index of a substance; (2) crystal tests: treatment of a substance with a chemical reagent to produce crystals; (3) chemical spot tests: treatment with a chemical reagent producing color changes; (4) chromatographic tests (thin layer or gas): these separate the mixtures under investigation. Confirmatory tests generally involve mass spectrometry in combination with gas chromatography. Every toxin has a characteristic mass spectrum that identifies it absolutely.

Drugs analysis in tissue samples can be very complicated and a substance under analysis must be subjected to rigorous tests with no margin for error. A range of screening tests employing color reactions exist for the detection of illegal drugs. Some commonly used color tests include the Marquis test for opium, Duquoin-Levine test for Marijuana, Van Urk test for LSD, Scott test for cocaine, and Dillie-Koppanyi test for barbiturates.

The challenges of modern science call on clinical and forensic toxicologists to expand their services. They are now encouraged to engage in research and development to meet a number of changing needs. Modern molecular biology has opened up a number of interesting possibilities for toxicologists. For example, genotyping for interpretation of potential toxic drug interactions and criminality testing is becoming a field of great interest. With the emergence of pharmacogenetics, genotyping may enhance rational drug therapy for better patient care, and may explain unexpected adverse or fatal drug reactions in postmortem analysis.

Expanding responsibilities for forensic toxicologists also derive from the greater threat of terrorism. Terrorism via weapons of mass destruction has moved out from war zones to civilian settings. Modern terrorist weapons may be in the form of nuclear, biological, and chemical devices. Recently, the possible use of chemical or biological weapons in the Middle East conflicts, the use of sarin gas in a Tokyo subway station, and the unregulated availability of nuclear fuel in some countries have all heightened the potential risks. Toxicologists must now be knowledgeable about the clinical pharmacology, safe samples processing, and possible screening and/or analysis of substances such as vesicants, cyanide, nerve agents, and riot control agents.

#### ■ FURTHER READING:

##### BOOKS:

- Bodziak, J., and Jon J. Nordby. *Forensic Science: An Introduction to Scientific and Investigative Techniques*. CRC Press, 2002.
- Klaassen, C. D. *Toxicology: The Basic Science of Poisons*. McGraw-Hill Companies, 2001.

## PERIODICALS:

- Goldberger, B. A., and A. Poletini. "Forensic Toxicology: Web Resources." *Toxicology* 173 (2002): 97–102.
- Maurer H. H. "Liquid Chromatography-mass Spectrometry in Forensic and Clinical Toxicology." *J Chromatogr B Biomed Sci Appl.* 713 (1998): 3–25.
- Richardson T. "Pitfalls in Forensic Toxicology." *Ann Clin Biochem.* 37 (2000): 20–44.
- Thormann, W., Y Aebi, M. Lanz, and J. Caslavka "Capillary Electrophoresis in Clinical Toxicology." *Forensic Sci Int.* 92 (1998): 157–83.
- Wong, S. H. "Challenges of toxicology for the millennium." *Ther Drug Monit.* 22 (2000): 52–7102.

## SEE ALSO

*Chemical and Biological Detection Technologies*  
*Chemistry: Applications in Espionage, Intelligence, and Security Issues*  
*Drug Control Policy, United States Office of National Forensic Science*  
*Thin Layer Chromatography*

---

## Toxins

---

■ BRIAN HOYLE

Toxins are compounds that are produced and released by a variety of microorganisms and other organisms. Toxins can be fast-acting and, because they are already preformed, do not require the growth of a microorganism in the host. State-sanctioned weaponization programs for various toxins have occurred in the past in many countries, and may be ongoing. As well, toxins are a potent weapon for terrorists.

**Bacterial toxins.** Toxins are the main disease-causing factor for a number of bacteria. Some examples include *Corynebacterium diphtheriae* (diphtheria), *Vibrio cholerae* (cholera), *Bacillus anthracis* (anthrax), *Clostridium botulinum* (botulism), certain strains of *Escherichia coli* (hemolytic uremic syndrome), and *Staphylococcus aureus* (toxic shock syndrome).

Certain species of these bacteria are of particular concern in biological warfare and biological terrorism. As the events of 2001 in the United States demonstrated, powdered preparations of *Bacillus anthracis* spores was easily delivered to a target through the mail. The dispersal of the spores in the air and the inhalation of the spores can cause a form of anthrax that develops quickly and, without treatment, is almost always fatal. The bacteria in the genus *Clostridium* also form spores. Additionally, during the 1990s, a strain of *Staphylococcus aureus* emerged that is resistant to almost all known antibiotics.

Bacterial toxins have a wide variety of activity. Some toxins damage the cell wall of host cells, either by dissolving the wall or by chemically punching holes through the wall. Examples of such toxins are the alpha toxin of *Clostridium perfringens*, hemolysin of *Escherichia coli*, and streptokinase of *Streptococcus pyogenes*. The damage to the host cells allows the bacteria to spread rapidly through the host. This can cause an overwhelming infection.

Other bacterial toxins kill host cells by stopping the manufacture of protein in host cells or by degrading the proteins. Examples of protein blockers include exotoxin A of *Pseudomonas aeruginosa* and the Shiga toxins produced by both *Escherichia coli* and *Shigella dysenteriae*. Protein degrading toxins include those produced by *Bacillus anthracis* and *Clostridium botulinum*.

Still other toxins stimulate an immune response of the host that is so strong that it can damage the host. *Staphylococcus aureus* produces at least three different toxins that have this effect (i.e., toxic shock syndrome).

**Marine toxins.** Microorganisms called dinoflagellates can produce toxins when they grow in species of shellfish. Usually, the toxins are a concern when the contaminated seafood is inadvertently eaten. But, the toxins can be isolated in pure form. The purified toxins will produce illness when deliberately used.

**Aflatoxin.** Aflatoxin is produced by two species of mold—*Aspergillus flavus* and *Aspergillus parasiticus*. The toxin is especially a concern when potatoes are contaminated by the mold. Ingestion of the contaminated potatoes can cause serious, even fatal illness. This toxin is of particular concern for food supplies. Storehouses of produce like potatoes are susceptible to the malicious release of the molds.

**Ricin.** Ricin is a toxin that is produced by the castor bean. It is the third most deadly toxin that is known, after the toxins produced by *Clostridium botulinum* and *Clostridium tetani*. The symptoms of ricin toxin include nausea, muscle spasms, severe lung damage, and convulsions. These symptoms appear within hours, and, without treatment, death from pulmonary failure can result within three days. There is no vaccine or antidote for the toxin.

Ricin has long been a weapon of espionage and terrorism. The most famous use of ricin occurred in 1978, when Georgi Markov—a recently defected Bulgarian official—was killed by KGB agents on a bridge in London. An umbrella tip was used to inject a capsule of ricin into one of his legs.

The planned use of ricin by al-Qaeda has been alleged. Traces of ricin have been found in caves in Afghanistan that were used by al-Qaeda. Iraq is also suspected of using ricin in its weaponization program of the 1990s.

Also, in January 2003, British antiterrorism officers seized a quantity of ricin in London from a group of Algerian men suspected of being terrorists.

**Toxoid vaccines.** Some toxins that are capable of causing much harm are also a source of protection. Because of its potency, a toxin cannot be used protectively in its unaltered form. Toxins can be altered, however, so that they do not produce the undesirable effects, but which still stimulate the immune system to produce antibodies to a critical part of the toxin molecule. The weakened version of a toxin is called a toxoid.

The anthrax vaccine that is currently licensed for use contains two toxoids in addition to other immune stimulating molecules. The immune response will produce antibodies to the two toxins of the anthrax bacterium.

#### ■ FURTHER READING:

##### PERIODICALS:

Schmitt, C. K., K. C. Meysick, and A. D. O'Brien. "Bacterial Toxins: Friends or Foes?" *Emerging Infectious Diseases* no. 5 (1999): 224–34.

##### ELECTRONIC:

Centers for Disease Control and Prevention. "Marine Toxins." Division of Bacterial and Mycotic Diseases. June 10, 2002. <[http://www.cdc.gov/ncidod/dbmd/diseaseinfo/marinetoxins\\_g.htm](http://www.cdc.gov/ncidod/dbmd/diseaseinfo/marinetoxins_g.htm)>(29 January 2003).

United States Department of Agriculture. "Aflatoxin." USDA Grain Inspection, Packers and Stockyards Administration. September 17, 1998. <<http://www.usda.gov/gipsa/newsroom/backgrounders/b-aflatox.htm>>(29 January 2003).

University of Wisconsin at Madison. "Mechanisms of Bacterial Pathogenicity: Protein Toxins." Bacteriology at UW-Madison. 2002. <<http://www.bact.wisc.edu/Bact330/lecturept>>(30 January 2003).

##### SEE ALSO

*Biocontainment Laboratories*  
*Biosensor Technologies*  
*Food Supply, Counter-terrorism*

information to the officer, the method for paying the agent, and the many precautions and tactics of deception applied along the way.

Examples of tradecraft can be found in the Ashenden stories, through which British author Somerset Maugham recounted, in fictional form, his experiences as a spy in World War I. In one tale, for instance, Maugham mentioned that Ashenden met an "old butter-woman" regularly in a market in Geneva. The woman was actually an agent of British intelligence who, in real life, passed notes back and forth between Maugham and his superiors in London. This is tradecraft in its simplest form—the employment of someone or something that is not exactly who or what he/she/it seems to be.

Another example of tradecraft in action is the artwork of Robert Baden-Powell who, long before he founded the Boy Scouts, served as a military intelligence officer in the Balkans during the 1890s. In order to sketch enemy fortifications without attracting attention, Baden-Powell adopted the disguise of an entomologist. He made detailed sketches of butterflies and leaves that, on close scrutiny, were revealed to be maps of gun emplacements or trenches.

Tradecraft can also include the many precautions taken to avoid detection in the process of making a drop, or otherwise transferring material between agent and officer, as in Maugham's case of the old butter-woman. In real life, Soviet agent John made his drops using a garbage bag that included bits of recognizable trash—but nothing that would smell strongly, attract animals, or cause damage to the documents and other important materials he left for his KGB handlers.

#### ■ FURTHER READING:

##### BOOKS:

Carl, Leo D. *The CIA Insider's Dictionary of U.S. and Foreign Intelligence, Counterintelligence, and Tradecraft*. Washington, D.C.: NIBC Press, 1996.

Melton, H. Keith. *The Ultimate Spy Book*. New York: DK Publishing, 1996.

Nash, Jay Robert. *Spies: A Narrative Encyclopedia of Dirty Deeds and Double Dealing from Biblical Times to Today*. New York: M. Evans, 1997.

Polmar, Norman, and Thomas B. Allen. *Spy Book: The Encyclopedia of Espionage*. New York: Random House, 1998.

##### SEE ALSO

*Cambridge University Spy Ring*  
*Cameras*  
*Cameras, Miniature*  
*Concealment Devices*  
*Dead Drop Spike*  
*Dead-Letter Box*  
*Hanssen (Robert) Espionage Case*  
*Intelligence Agent*  
*Intelligence Officer*  
*Walker Family Spy Ring*

## Tradecraft

Operatives of intelligence services and other covert organizations use the term *tradecraft* to refer to the techniques of the espionage trade, or the methods by which an agency involved in espionage conducts its business. Elements of tradecraft, in general terms, include the ways in which an intelligence officer arranges to make contact with an agent, the means by which the agent passes on





United States soldiers, left, stand watch in Grand Central Terminal in New York after the Transportation Department warned transit and other railroad systems about possible terrorist attacks in May 2002. AP/WIDE WORLD PHOTOS.

## Transportation Department, United States

A vital part of America's critical infrastructure, the United States Department of Transportation (DOT) was established by an act of Congress in 1966 and began operation on April 1, 1967. Today the DOT comprises a number of bureaus and offices designed to promote efficiency and safety in air, road, rail, and marine travel and transport throughout the nation. The mission of DOT is to develop and coordinate policies to provide efficient, economical national transport systems whose operations take into account economic, environmental, and national security needs.

**Agencies of DOT.** In addition to the Office of the Secretary, DOT consists of 11 individual operating agencies. Among these are the Federal Aviation Administration, which oversees the safety of civil air transport. DOT was also home to the Transportation Security Administration, created in the wake of the 2001 terrorist attacks to provide

aviation security, and the U.S. Coast Guard. Both were transferred to the newly created Department of Homeland Security in March 2003. Sea borne components of DOT include the Maritime Administration, which promotes the development and maintenance of the U.S. merchant marine, and the Saint Lawrence Seaway Development Corporation, which maintains the waterway between the Great Lakes and Atlantic Ocean.

Areas of DOT devoted to highways and railroads include the Federal Highway Administration, which coordinates inter- and intrastate highway programs and manages roads on federal lands such as national forests and Indian reservations; the Federal Motor Carrier Safety Administration, established in 2000 to reduce commercial motor vehicle-related fatalities and injuries; the Federal Railroad Administration, which promotes safe and environmentally sound rail transport; the Federal Transit Administration, which assists cities and communities in developing and improving mass transit systems; and the National Highway Traffic Safety Administration, which is responsible for reducing deaths and economic losses from motor vehicle crashes.

Other agencies of DOT are the Research and Special Programs Administration, which oversees the transport of

hazardous materials; the Bureau of Transportation Statistics, which collects data on transport and travel, and works closely with the Bureau of the Census in the Commerce Department; and the Surface Transportation Board, which is responsible for economic regulation of interstate surface transportation, primarily railroads. The last of these is an independent body organizationally housed within DOT.

#### ■ FURTHER READING:

##### BOOKS:

- National Transportation Strategic Research Plan*. Washington, D.C.: National Science and Technology Council, 2000.
- U.S. Department of Transportation Research and Development Plan*. Washington, D.C.: John A. Volpe National Transportation Systems Center, 1999.
- Whitnah, Donald Robert. *U.S. Department of Transportation: A Reference History*. Westport, CT: Greenwood Press, 1998.

##### ELECTRONIC:

- U.S. Department of Transportation. <<http://www.dot.gov/>> (April 3, 2003).

##### SEE ALSO

- Air Marshals, United States*  
*Aviation Security Screeners, United States*  
*Civil Aviation Security, United States*  
*Coast Guard (USCG), United States*  
*Critical Infrastructure*  
*FAA (United States Federal Aviation Administration)*  
*Homeland Security, United States Department*  
*NTSB (National Transportation Safety Board)*  
*Port Security*

## Treasury Department, United States

#### ■ MARTIN J. MANNING

The United States Department of the Treasury, the second-oldest department in the U.S. Government, was established by an Act of Congress on 2 September 1789 (1 Stat. 65; 31 U.S.C. 1001). It advises Congress and the president on tax policy, acts as financial agent for the federal government, manufactures currency, and enforces tax laws. According to its establishment legislation, the Treasury Department is to “formulate, recommend, and administer domestic and international financial, economic, and tax policies, and manage the public debt.” The Department serves as the principal financial agent for the United States government, manufactures coins and currency,

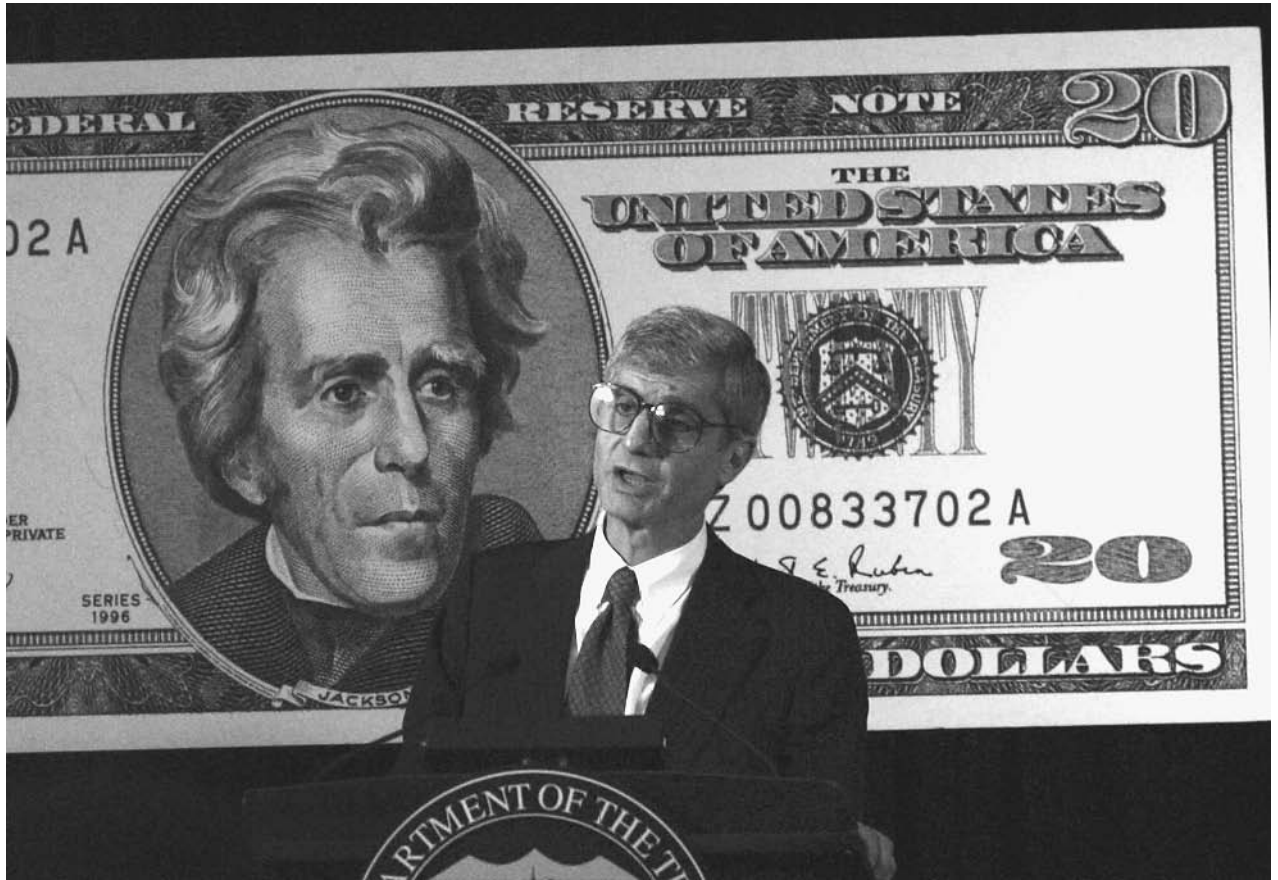
and oversees the administration of the U.S. Customs Service (1789), U.S. Mint (1792), Internal Revenue Service (1862), Bureau of Engraving and Printing (1862), Office of the Comptroller of the Currency (1863), Secret Service (1865), Bureau of the Public Debt (1919), Financial Management Service (1920), Federal Law Enforcement Training Center (1970), Bureau of Alcohol, Tobacco, and Firearms (1972), and Office of Thrift Supervision (1989).

**Background.** The Treasury Department was already in existence in some form during the War of American Independence. On June 22, 1775, the Second Continental Congress approved the printing of \$2 million in bills of credit to finance the War of American Independence. Between 1775 and 1779, more than \$241 million Continentals were issued. The value of this first national paper money fell so low it engendered the expression “not worth a Continental.” A month later, July 29, 1775, the Continental Congress appointed joint treasurers (Michael Hillegas and George Clymer). That November, a committee was established by the Continental Congress to examine the money in the Treasury and to estimate the public debt. The committee was one of several established by the Congress to handle different phases of the revolutionary finances. In February 1776, a standing committee of five was appointed to superintend the Treasury. The committee was referred to by various names, including Board of Treasury and Treasury Office of Accounts.

On July 31, 1789, the collection of customs revenue was established when the Tariff Act became effective. A Bureau of Customs, later the U.S. Customs Service, was created by an act of March 3, 1927 (44 Stat. 1381); 19 U.S.C. 2071). A postal service was established by Congress on September 22, 1789.

With the establishment of the Treasury Department, the first Secretary of the Treasury, Alexander Hamilton, maneuvered to give the emerging United States a strong financial basis and to provide the stability needed for economic development. Hamilton worked to fund the national debt, assume the state debts, create a national bank, pass a whiskey tax, enact high tariffs, and establish American industry on a sound financial footing. He was aided by legislation (April 2, 1792) that established a national mint and regulated coinage and an act (May 8, 1792; revised Act of March 3, 1809, chap. 28) that organized the Department of the Treasury into two major components: the Departmental offices, primarily responsible for the formulation of policy and management of the Department as a whole, and the operating bureaus, which carry out the specific operations assigned to the Department. Today, the bureaus make up 98% of the Treasury work force.

**Key developments.** Congress approved legislation (June 23, 1836) that required the Secretary of the Treasury to designate at least one bank in each state and territory for the



Treasury Secretary Robert Rubin holds a 1998 press conference to announce the release of a new \$20 bill, redesigned to include features that make it more difficult to counterfeit. Anti-counterfeit features will be enhanced every seven to ten years, and will include subtle color changes. AP/WIDE WORLD PHOTOS.

deposit of government funds. Six years later, on Independence Day, sub-treasuries for deposit of federal funds were authorized in major cities but the legislation was repealed the next year (1841).

The Civil War (1861–1865) was the first modern war demanding enormous capital. The cost, after four years, was \$2.3 billion to the U.S. government and \$1 billion to the Confederacy. Less than one-fifth of the North's cost was paid for in taxes; four-fifths was financed by borrowing and the issue of unredeemable paper currency. To remedy this, and to set up future reserves, the Revenue Act (12 Stat. 432; 26 U.S.C. 3900; July 1, 1862) established a permanent tax collection agency, Commissioner of Internal Revenue, although internal taxes were levied by Congress and collected by the Treasury Department from 1791 to 1802 and 1813 to 1817. To administer the national banks, the Office of the Comptroller of the currency was created by legislation (12 Stat. 665; February 25, 1863). However, a national tragedy led to the creation of one of the better-known Treasury bureaus when the U.S. Secret Service, oldest general law enforcement agency in the federal government, was established (July 5, 1865) after the Lincoln assassination. Along with its protection of presidential families, heroically documented in stage

screen, and print, the Secret Service was also authorized to halt the counterfeiting of currency. It derives its authority from the act of June 23, 1860 (12 Stat. 102). Today, it still provides these services although its detection of counterfeit money and its arrest of counterfeiters continues to fall behind its rather more popular and visual image of Secret Service agents traveling with the president and other VIPs.

**“Guns and Butter” diplomacy.** World War I cost \$32.7 billion. To finance this enormous cost, President Wilson and Treasury Secretary William G. McAdoo transformed the income tax into the foremost instrument of federal taxation, both to raise revenue and to attack concentrations of wealth, special privilege, and public corruption; and to promote a more competitive economy. The Revenue Acts (1916, 1917) [39 Stat. 756, 1000] imposed the first significant taxes on corporate profits and personal incomes and introduced a graduated federal estate tax, but rejected a mass-based income tax. An excess profits tax became the centerpiece of wartime finance.

Henry Morgenthau, President Franklin Roosevelt's Secretary of the Treasury, issued regulations in 1934 that established a reporting system for specified international

capital movements. Along with the required reports on security and foreign exchange transactions and changes in bank balances between the United States and foreign countries, commercial and industrial firms reported their foreign assets and liabilities. The present Treasury International Capital reporting system, an ongoing statistical program, evolved from the 1934 data collection efforts.

World War II, the most costly in American history at \$360 billion, changed the American tax system as it shifted from a narrow base to a broad base, the basis of our current tax system. Roosevelt and Morgenthau wanted to finance the war with taxes that came mostly from business and upper-income groups as nearly one-half of America's national product went to war. Along with lend-lease programs, Treasury designed and implemented Foreign Funds Control (1940) to protect in the U.S. the assets of invaded countries and to keep them from the enemy. Foreign Funds Control froze Axis assets in 1941, regulated international financial transactions, administered wartime trade restrictions (Trading with the Enemy Act), and froze \$8.5 billion of assets belonging to thirty-five countries by war's end. Although liquidated in 1948, Foreign Funds Control was re-established in 1950 as Foreign Assets Control.

Production of military invasion currency was among the Treasury's most highly secret work since any knowledge of production would reveal Allied invasion plans. Treasury loaned 14,000 tons of silver to help produce uranium for the atom bomb and financed the top-secret Manhattan Project while Morgenthau and a group of Treasury attorneys persuaded Roosevelt to establish the War Refugee Board (1944), the only government effort to save European Jews.

In the post-World War II period, Treasury developed international monetary policy to aid countries devastated by the war but by the end of the Korean War, the U.S. American dominance was lessening as it began to compete for economic control with countries it originally assisted. Treasury, supported by other U.S. agencies, developed comprehensive proposals for the reform of the international monetary system after fiscal collapses in the 1960s and the 1970s. Strengthened by accords and agreements, Treasury developed further policies to resolve the international debt crises of the 1980s and the early 1990s. Since 1989, Treasury has guided U.S. participation in the Financial Services negotiations of the Uruguay Round multilateral talks under the General Agreement on Trade in Services and the World Trade Organization.

After the terrorist attacks of September 11, 2001, the Treasury Department implemented regulations for helping financial institutions comply with the USA PATRIOT Act, a comprehensive legislative enactment addressing many facets of terrorist financing and money laundering passed by Congress after the terrorist attacks. The Department works jointly with other federal agencies to craft effective and common-sense regulations and programs that will help industry guard against future terrorist infiltration and abuse.

To date, the Treasury Department has issued a number of proposed and interim rules to help the financial services industry address specific threats to the financial system, create anti-money laundering programs that are tailored to each industry's needs, alert the appropriate authorities to large or suspicious financial transactions, and better understand their relationship with foreign banks. At the beginning of the twenty-first century, Treasury continues to maintain a central position within the federal government due to its size, leadership, and important role in the economic development of the United States.

#### ■ FURTHER READING:

##### BOOKS:

- Gilbert, Abby L. "Treasury, Department of the." In: Kurian, George T., ed. *A Historical Guide to the U.S. Government*. New York and Oxford: Oxford University, 1998.
- Katz, Bernard S., and C. Daniel Vencill, eds. *Biographical Dictionary of the United States Secretaries of the Treasury, 1789–1995*. Westport, CT: Greenwood, 1996.
- Walston, Mark. *The Department of the Treasury*. New York: Chelsea House, 1989.

##### ELECTRONIC:

- U.S. Department of the Treasury Department <<http://www.ustreas.gov>> (April 18, 2003).

##### SEE ALSO

- Internal Revenue Service, United States*  
*Secret Service, United States*

---

## Truman Administration (1945–1953), United States National Security Policy

---

#### ■ CARYN E. NEUMANN

The onset of the Cold War during the presidency of Harry S. Truman led the executive branch recognize a need to integrate domestic, foreign, and military policies to combat the expansionism of the Soviet Union. The Truman Doctrine set the major goal of the U.S. as opposition to communism anywhere in the world. The Marshall Plan, the Organization of American States (OAS), and the National Security Council (NSC) all served as part of the administration's unified approach to the immense challenges posed by the expansion of communism.

Harry S. Truman took office upon the sudden death of Franklin D. Roosevelt in April 1945. The new president

continued with much of the Roosevelt administration's diplomacy, but had always been far sterner than Roosevelt toward the Soviet Union. He also had to plan for a postwar world and the primary concern of the postwar Truman administration was to prevent a repeat of the Great Depression. American officials held that another economic downturn could only be avoided if global markets and raw materials were fully open to all peoples on the basis of equal opportunity. On the other hand, Josef Stalin, dictator of the Soviet Union, demanded that the U.S. recognize the Soviet right to control large parts of Eastern Europe. These Soviet satellite states would serve as a strategic buffer against the West that could also be exploited economically for the rapid rebuilding of the devastated Soviet economy. Truman refused to comply with the wishes of the Soviets and the Cold War gradually took root.

By 1946, the administration had become deeply concerned about the consolidation and development of Russian power. One year later, in 1947, Truman issued a declaration that would serve as the guiding force of national security policy for the duration of the Cold War. With the Truman Doctrine, he asked Americans to join in a global fight against communism. He committed the U.S. to opposing totalitarian regimes and supporting freedom, while refusing to place any geographical limits upon this obligation. Several days after the speech, the president announced a loyalty program to ferret out security risks in government. The first such peacetime program in U.S. history, it was so vaguely defined that political ideas and long-ago associations were suddenly made suspect.

The overwhelming fear of communism at home and abroad would convince Americans to support a national security policy that included intervention in the affairs of other countries. The end of World War II confronted the United States with the problem of reconstructing Europe. Most of Europe lay in shatters, with countries too weak to readily rebuild the infrastructure necessary for economic growth. In order to prevent a collapse of the European economy and the ramifications on the economy of America, the Truman administration began a massive economic aid effort. The 1948 Marshall Plan, named for Secretary of State George C. Marshall, offered aid to all of Europe with the provision that the Europeans determine their own needs. Before its end in 1951, the plan prevented poverty and chaos from overwhelming Western Europe. The Soviets, suspicious of American aims, declined to participate.

In order to prevent communist aggression around the world, the U.S. joined with its neighbors to the south in a mutual security agreement. The nations of the Western Hemisphere convened in Rio de Janeiro, Brazil in 1947 to sign the Rio Treaty for collective self-defense. The agreement provided that an attack upon one nation in the Americas served as an attack upon them all. If two-thirds of the countries agreed to resist an attack, all states must cooperate by sending either troops or supplies. In 1948,

the U.S. participated in the formation of the Organization of American States (OAS). The administration hoped that the OAS would eventually assume the mounting responsibilities for solving hemispheric problems, but the U.S. would always play the dominant role.

By 1947, the various means of security planning had fully emerged and ranged from economic planning through diplomatic initiative to application of military force. The missing element was a forum in which to select the appropriate combination of measures for a particular situation. Truman generally relied upon Special White House Counsel Clark Clifford to provide day-to-day coordination. Clifford, dismayed by the disorder among agencies involved in major policymaking decisions, played an instrumental role in establishing the National Security Council in 1947 to give institutional stability to national security policymaking.

Until the advent of the Korean War in 1950, Truman remained unenthusiastic about the NSC. Truman saw the NSC as an effort by Congress to harness the president to the advice of military men. He attended only 10 of the first 55 meetings on the grounds that his presence would inhibit frank discussion and suggest that national policies were made by committee. When Truman did participate in NSC gatherings, the council reached conclusions that matched his known desires and ideological inclinations. The complicated situation in war-torn Korea finally convinced Truman of the value of the NSC as a policy development mechanism.

During the Truman administration, the NSC's main products were policy papers. NSC-20/4 served as the basic American strategic plan from 1948 until 1950. This document saw Russian expansionism as part of a massive drive for world mastery. It stated that the U.S. would not attempt an occupation of the Soviet Union but should be prepared for a negotiated peace. American objectives were set as the reduction of the power and influence of the Soviet Union to the point where the U.S.S.R. could no longer mount a threat to world peace.

NSC-68, the replacement for NSC-20/4, is arguably among the most significant of NSC documents. In it, the NSC argued that in the current polarized climate, a defeat of free institutions anywhere in the world damaged the U.S. This belief defined any threat to the capitalist political system as communist-inspired, not as the result of problems within. NSC-68 shocked the government into greater anti-communist resolution and action, thereby setting the stage for involvement in wars in Korea and Vietnam. It also comprised the final attempt of the Truman administration to define national security policy.

In establishing the national security policy and system that would guide the United States for much of second half of the twentieth century, Truman opened the Cold War. Fear of communism and determination to oppose it at every opportunity led to the U.S. involvement in the Korean War as well as McCarthyism.

## ■ FURTHER READING:

### BOOKS:

Boll, Michael M. *National Security Planning: Roosevelt through Reagan*. Lexington: University Press of Kentucky, 1988.

Crabb, Cecil V., and Kevin V. Mulcahy. *American National Security: A Presidential Perspective*. Pacific Grove, CA: Brooks/Cole, 1991.

Graebner, Norman A., ed. *The National Security: Its Theory and Practice, 1945–1960*. New York: Oxford University Press, 1986.

### ELECTRONIC:

White House. "History of the National Security Council, 1947–1997" <<http://www.whitehouse.gov/nsc/history.html>> (April 25, 2003).

### SEE ALSO

*Cold War (1945–1950), The Start of the Atomic Age*

*Cold War (1950–1972)*

*Department of State, United States*

*Korean War*

*McCarthyism*

*National Security Act (1947)*

*NSC (National Security Council)*

*National Security Strategy, United States*

## Truman Doctrine.

SEE *Cold War (1950–1972)*.

## Truth Serum

### ■ BELINDA ROWLAND

Truth serum is a term given to any of a number of different sedative or hypnotic drugs that are used to induce a person to tell the truth. Truth serums cause a person to become uninhibited and talkative, but they do not guarantee the veracity of the subject.

In 1943, J. Stephen Horsley published a book in which he described the psychotherapeutic method of narcoanalysis. By chance, he observed that persons who were under the influence of narcotics were uninhibited, talkative, and answered all questions that were asked of them. A narcotic is a drug that dulls the senses, relieves pain, and induces sleep. Persons who were under the influence of narcotics entered a hypnotic-like state and spoke freely about anxieties or painful memories. Once the drug effect had worn off, the person had no recollection of what he or she said. Horsley coined the term "narcoanalysis." Narcoanalysis has since been used to assist in the diagnosis of several different psychiatric conditions.

The term "truth serum" has been applied to drugs that are used in narcoanalysis. This term is a misnomer in two ways: the drugs used are not serums and truthfulness is not guaranteed. Although inhibitions are generally reduced, persons under the influence of truth serums are still able to lie and even tend to fantasize. Courts have ruled that information obtained from narcoanalysis is inadmissible.

Narcoanalysis is not used in the United States as an interrogation method. The Federal Bureau of Investigation (FBI) and other federal law enforcement agencies object to the use of truth drugs, preferring instead to use psychological methods to extract information from suspects or prisoners. The United Nations considers the use of truth drugs to be physical abuse and, therefore, a form of torture. The issue was revisited in 2002, when some authorities, including former Central Intelligence Agency and FBI chief William Webster, frustrated by the lack of forthcoming information from suspected al-Qaeda and Taliban members held at the U.S. prison in Guantanamo Bay, Cuba, advocated administering narcoanalysis drugs to uncooperative captives. United States Secretary of Defense Donald Rumsfeld asserted that narcoanalysis is not used by United States military and intelligence personnel, but suggested that other countries have made use of the technique in the interrogation of suspected terrorists.

**Drugs used as truth serums.** Two of the most commonly used truth serums are members of the barbiturate drug class. Barbiturates are sedatives and hypnotics that are created from barbituric acid. They are divided into classes according to the duration of sedation: ultrashort, short, intermediate, and long. Ultrashort-acting barbiturates are used as anesthetics whereas long-acting ones are used to treat convulsions (anticonvulsive). Barbiturates are controlled substances due to their high potential for abuse and for addictive behavior.

Sodium pentothal (pentothal sodium, thiopental, thiopentone) is an ultrashort-acting barbiturate, meaning that sedation only lasts for a few minutes. Sodium pentothal slows down the heart rate, lowers blood pressure, and slows down (depresses) the brain and spinal cord (central nervous system) activity. Sedation occurs in less than one minute after injection. It is used as a general anesthetic for procedures of short duration, for induction of anesthesia given before other anesthetic drugs, as a supplement to regional anesthesia (such as a spinal block), as an anticonvulsive, and for narcoanalysis.

Sodium amytal (amobarbital, amylobarbitone, Amytal) is an intermediate-acting barbiturate. Sedation occurs in one hour or longer and lasts for 10 to 12 hours. Sodium amytal depresses the central nervous system. It is used as a sedative, hypnotic, and anticonvulsive and for narcoanalysis. When sodium amytal is used for narcoanalysis it may be called an "Amytal interview."

Scopolamine (hyoscine) is an anticholinergic alkaloid drug that is obtained from certain plants. Anticholinergic

drugs block the impulses that pass through certain nerves. Scopolamine affects the autonomic nervous system and is used as a sedative, to prevent motion sickness, to treat eye lens muscle paralysis (cycloplegic), and to dilate the pupil (mydriatic).

#### ■ FURTHER READING:

##### BOOKS:

Horsley, J. Stephen. *Narco-Analysis. A New Technique in Short-Cut Psychotherapy: A Comparison with Other Methods and Notes on the Barbiturates*. New York: Oxford University Press, 1943.

##### PERIODICALS:

Johnson, K. and R. Willing. "Ex-CIA Chief Revitalizes 'Truth Serum' Debate." *USA Today*. (April 26, 2002): 12a.

Romanko, J.R.. "Truth Extraction." *New York Times Magazine*. (November 19, 2000): 54.

##### SEE ALSO

*Polygraphs*

## Tularemia

■ BRIAN HOYLE

Tularemia is a plague-like disease caused by the bacterium *Francisella tularensis*. U.S. weapons stores of tularemia bacteria were reported destroyed in 1973. Until the demise of the Soviet Union, its biological weapons development program actively developed strains of the bacterium that were resistant to antibiotics and vaccines. As of March 2003, the whereabouts and disposition of some Soviet era tularemia stocks remains uncertain.

Tularemia is listed as potential bioterrorist weapon because it is easily obtained and potentially lethal.

World Health Organization (WHO) estimates hypothesize that if 50 kg of "weaponized" or highly virulent bacterium *Francisella tularensis* was dispersed in aerosol form over a large city, depending on weather and exposure patterns, there could be as many as 250,000 infections resulting in a projected 19,000 deaths.

Tularemia bacterium is transferred to humans from animals (i.e., a zoonosis) such as rodents, voles, mice, squirrels, and rabbits. Reflecting the natural origin of the disease, tularemia is also known as rabbit fever. Indeed, the rabbit is the most common source of the disease. Transfer of the bacterium via contaminated water and vegetation is possible as well.

The disease can easily spread from the environmental source to humans (although direct person-to-person contact has not been documented). This contagiousness and the high death rate among those who contract the

disease made the bacterium an attractive bioweapon. Both the Japanese and Western armies experimented with *Francisella tularensis* during World War II. Experiments during and after that war established the devastating effect that aerial dispersion of the bacteria could exact on a population.

Tularemia naturally occurs over much of North America and Europe. In the United States, the disease is predominant in south-central and western states such as Missouri, Arkansas, Oklahoma, South Dakota, and Montana. The disease almost always occurs in rural regions. The animal reservoirs of the bacterium become infected typically by a bite from a blood-feeding tick, fly, or mosquito.

The causative bacterium, *Francisella tularensis* is a Gram-negative bacterium that, even though it does not form a spore, can survive for protracted periods of time in environments such as cold water, moist hay, soil, and decomposing carcasses.

The number of cases of tularemia in the world is not known, as accurate statistics have not been kept, and because illnesses attributable to the bacterium go unreported. In the United States, the number of cases used to be high. In the 1950s, thousands of people were infected each year. This number has dropped considerably, to less than 200 each year, and those who are infected now tend to be those who are exposed to the organism in its rural habitat (e.g., hunters, trappers, farmers, and butchers).

Humans can acquire the infection through breaks in the skin and mucous membranes, by ingesting contaminated water, or by inhaling the organism. An obligatory step in the establishment of an infection is the invasion of host cells. A prime target of invasion is the immune cell known as macrophages. Infections can initially become established in the lymph nodes, lungs, spleen, liver, and kidney. As these infections become more established, the microbe can spread to tissues throughout the body.

Symptoms of tularemia vary depending on the route of entry. Handling an infected animal or carcass can produce a slow-growing ulcer at the point of initial contact and swollen lymph nodes. When tularemia is inhaled, the symptoms include the sudden development of a headache with accompanying high fever, chills, body aches (particularly in the lower back) and fatigue. Ingestion of the organism produces a sore throat, abdominal pain, diarrhea, and vomiting. Other symptoms can include eye infection and the formation of skin ulcers. Some people also develop pneumonia-like chest pain. An especially severe pneumonia develops from the inhalation of one type of the organism, which is designated as *Francisella tularensis biovar tularensis* (type A). The pneumonia can progress to respiratory failure and death. The symptoms typically tend to appear three to five days after entry of the microbe into the body.

The infection responds to antibiotic treatment and recovery can be complete within a few weeks. Recovery produces a long-term immunity to re-infection. Some

people experience a lingering impairment in the ability to perform physical tasks. If left untreated, tularemia can persist for weeks, even months, and can be fatal. The severe form of tularemia can kill up to 60% of those who are infected if treatment is not given.

A vaccine is available for tularemia. To date this vaccine has been administered only to those who are routinely exposed to the bacterium (e.g., researchers). The potential risks of the vaccine, which is a weakened form of the bacterium, have been viewed as being greater than the risk of acquiring the infection.

#### ■ FURTHER READING :

##### BOOKS:

Chin, J. "Tularemia." In *Control of Communicable Diseases Manual*. Washington, DC: American Public Health Association, 2000.

Dennis, D. T. "Tularemia." In: Wallace, R. B. ed. *Maxcy-Rosenau-Last Public Health and Preventive Medicine*, 14th edition. Stamford: Appleton & Lange, 1998.

##### SEE ALSO

*Bioterrorism, Protective Measures Infectious Disease, Threats to Security*

## Tunisian Combatant Group (TCG)

The Tunisian Combatant Group (TCG) also operates as, or is known as, the Tunisian Islamic Fighting Group.

The TCG's goals reportedly include establishing an Islamic government in Tunisia and targeting Tunisian and Western interests. Founded probably in 2000 by Tarek Maaroufi and Saifallah Ben Hassine, the group has come to be associated with al-Qaeda and other North African Islamic extremists in Europe who have been implicated in anti-U.S. terrorist plots there during 2001. In December, Belgian authorities arrested Maaroufi and charged him with providing stolen passports and fraudulent visas for those involved in the assassination of Ahmed Shah Massoud, according to press reports. Tunisians associated with the TCG are part of the support network of the international Salafist movement. According to Italian authorities, TCG members there engage in false document trafficking and recruitment for Afghan training camps. Some TCG associates are suspected of planning an attack against the U.S., Algerian, and Tunisian diplomatic interests in Rome in January. Members reportedly maintain ties to the Algerian Salafist Group for Call and Combat (GSPC).

#### ■ FURTHER READING :

##### ELECTRONIC:

CDI (Center for Defense Information), Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <<http://www.cdi.org/terrorism/terrorist.cfm>> (April 17, 2003).

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001," Annual Report: On the Record Briefing. May 21, 2002 <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17,2003).

U.S. Department of State. Annual Reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

##### SEE ALSO

*Terrorism, Philosophical and Ideological Origins Terrorist and Para-State Organizations Terrorist Organization List, United States Terrorist Organizations, Freezing of Assets*

## Tupac Amaru Revolutionary Movement (MRTA)

Tupac Amaru Revolutionary Movement (MRTA) is a traditional Marxist-Leninist revolutionary movement formed in 1983 from remnants of the Movement of the Revolutionary Left, a Peruvian insurgent group active in the 1960s. The MRTA aims to establish a Marxist regime and to rid Peru of all imperialist elements (primarily U.S. and Japanese influence). Peru's counterterrorist program has diminished the group's ability to carry out terrorist attacks, and the MRTA has suffered from infighting, the imprisonment or deaths of senior leaders, and loss of leftist support. Several MRTA members remained imprisoned in Bolivia. MRTA members have previously conducted bombings, kidnappings, ambushes, and assassinations, but recent activity has fallen drastically. In December, 1996, 14 MRTA members occupied the Japanese Ambassador's residence in Lima and held 72 hostages for more than four months. Peruvian forces stormed the residence in April 1997, rescuing all but one of the remaining hostages and killing all 14 group members, including the remaining leaders. The group has not conducted a significant terrorist operation since and appears more focused on obtaining the release of imprisoned MRTA members.

MRTA is estimated to have fewer than 100 members, consisting largely of young fighters who lack leadership skills and experience. MRTA operates in Peru with supporters throughout Latin America and Western Europe.



## ■ FURTHER READING:

### ELECTRONIC:

CDI (Center for Defense Information), Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <<http://www.cdi.org/terrorism/terrorist.cfm>> (April 17, 2003).

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001," Annual Report: On the Record Briefing. May 21, 2002 <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual Reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

### SEE ALSO

*Terrorism, Philosophical and Ideological Origins*  
*Terrorist and Para-State Organizations*  
*Terrorist Organization List, United States*  
*Terrorist Organizations, Freezing of Assets*

## Turkey, Intelligence and Security

Turkey's intelligence service, MIT (Milli Istihbarat Teskilati; Special Organization) has roots that go back to the final years of the Ottoman Empire. Today, it is concerned largely with signals intelligence, and with monitoring threats from neighboring countries. Like most major industrialized nations, Turkey has a counterterrorism unit, the OIKB or National Police Jandarma Commandoes.

In 1914, Ottoman leader Enver Pasha established an intelligence service that became the Police Guild (Karakol Cemiyeti) after Turkey's defeat in World War I. In 1926, after Turkey emerged as a republic under the leadership of Ataturk (a.k.a. Mustafa Kemal), the Police Guild became MAH, the National Security Service. Directed by a former intelligence officer of imperial Germany, MAH conducted intelligence operations overseas, as well as counter-espionage work at home against Armenian and Kurdish separatists. In 1965, MAH became MIT, which has special sections devoted to internal security, counterterrorism, organized crime, Russia, Greece, Iraq, Kurdish separatists, and Cyprus.

Soldiers in OIKB are trained in aspects of riot control, hostage rescue, anti-hijacking operations, and other counterterrorism skills. Its members have conducted armed operations against Kurdish and Armenian rebels, as well as the Turkish People's Liberation Army. Controlled in peacetime by the Ministry of Interior, OIKB in wartime falls under the direction of military intelligence.

## ■ FURTHER READING:

### BOOKS:

Bennett, Richard M. *Espionage: An Encyclopedia of Spies and Secrets*. London: Virgin Books, 2002.

### PERIODICALS:

Dempsey, Judy. "EU Military Mission at Risk from Turkish Rift." *Financial Times*. (September 19, 2002): 12.

### ELECTRONIC:

Turkey: Intelligence. Federation of American Scientists. <<http://www.fas.org/irp/world/turkey/index.html>> (March 1, 2003).

### SEE ALSO

*Greece, Intelligence and Security*  
*Syria, Intelligence and Security*  
*NATO (North Atlantic Treaty Organization)*

## Turkish Hizballah

Turkish Hizballah is a Kurdish Islamic (Sunni) extremist organization that arose in the late 1980s in the Diyarbakir area in response to Kurdistan Workers' Party atrocities against Muslims in southeastern Turkey, where (Turkish) Hizballah seeks to establish an independent Islamic state. The group comprises loosely organized factions, the largest of which are Ilim, which advocates the use of violence to achieve the group's goals, and Menzil, which supports an intellectual approach. Beginning in the mid-1990s, Turkish Hizballah—which is unrelated to Lebanese Hizballah—expanded its target base and modus operandi from killing PKK militants to conducting low-level bombings against liquor stores, bordellos, and other establishments that the organization considered "anti-Islamic." In January 2000, Turkish security forces killed Huseyin Velioglu, the leader of (Turkish) Hizballah's Ilim faction, in a shootout at a safehouse in Istanbul. The incident sparked a year-long series of operations against the group throughout Turkey that resulted in the detention of some 2,000 individuals; authorities arrested several hundred of those on criminal charges. At the same time, police recovered nearly 70 bodies of Turkish and Kurdish businessmen and journalists that (Turkish) Hizballah had tortured and brutally murdered during the mid to late-1990's. The group began targeting official Turkish interests in January 2001, when 10–20 operatives participated in the assassination of the Diyarbakir police chief.

Turkish Hizballah operates primarily in southeastern Turkey—particularly the Diyarbakir region—and Turkish officials charge that the group receives at least some assistance, including training, from Iran. Turkish Hizballah strength is estimated at several hundred active members and several thousand supporters.

## ■ FURTHER READING:

### ELECTRONIC:

CDI (Center for Defense Information), Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <<http://www.cdi.org/terrorism/terrorist.cfm>> (April 17, 2003).

Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001," Annual Report: On the Record Briefing. May 21, 2002 <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. Annual Reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

### SEE ALSO

*Terrorism, Philosophical and Ideological Origins*  
*Terrorist and Para-State Organizations*  
*Terrorist Organization List, United States*  
*Terrorist Organizations, Freezing of Assets*

---

## Typex

---

Typex was the name for the principal encryption device, or cipher machine, used by the military, intelligence, and diplomatic services of the British Empire during World War II. In the 1920s, the British were still using book cipher systems, and became aware of the need to modernize using new cipher machinery. They initially planned to use the Enigma system, but instead settled on an improved Enigma machine known as "Type X." The Typex system remained in use among British forces throughout the war.

In 1926, the British government formed an interdepartmental committee to study technology as a means of finding a replacement for the laborious system of encryption by hand. For the purposes of evaluation, the government purchased two Enigma machines, but in January 1935, the committee advised the Royal Ministry to acquire three of the "Type X" machines, which represented an improved Enigma design. Satisfied with the machine, Whitehall commissioned the Creed & Company to manufacture Type X machines to specification.

As war broke out in September 1939, the British War Office and Air Ministry had fully adopted the Typex system, although the Royal Navy would continue to perform encryption by hand until 1943. Unlike the Germans, who encrypted nearly every official message on their Enigma machines, the British used their Typex system sparingly. This may have given them an unexpected advantage, because the Germans' proliferation of enciphered messages gave the British plenty of material to study. By contrast, the Germans made no significant attempt to crack the Typex ciphers, even though they captured several of the machines at Dunkirk and in North Africa.

Britain undertook the joint development of a Combined Cipher Machine with the Americans, who developed their own Sigaba system. In 1943, the Royal Navy began using the Combined Cipher Machine. Meanwhile, the rest of the British forces continued to use Typex, though British units in the China-Burma-India theatre adopted Sigaba, while some American units adopted Typex. After the war, many Typex machines remained in use among English-speaking nations for several decades until finally, in 1973, New Zealand became the last nation to set aside its Typex system.

## ■ FURTHER READING:

### BOOKS:

Freedman, Maurice. *Unravelling Enigma: Winning the Code War at Station X*. Barnsley, South Yorkshire, England: Leo Cooper, 2000.

Kozaczuk, Wladyslaw. *Enigma: How the German Machine Cipher Was Broken, and How It Was Read by the Allies in World War Two*. Frederick, MD: University Publications of America, 1984.

Melton, H. Keith. *The Ultimate Spy Book*. New York: DK Publishing, 1996.

Miller, A. Ray. *The Cryptographic Mathematics of Enigma*. Ft. Meade, MD: National Security Agency, 2001.

Polmar, Norman, and Thomas B. Allen. *Spy Book: The Encyclopedia of Espionage*. New York: Random House, 1998.

### SEE ALSO

*COMINT (Communications Intelligence)*

*Crib*

*Enigma*

*SIGINT (Signals intelligence)*

*Special Relationship: Technology Sharing Between the Intelligence Agencies of the United States and United Kingdom*

*Ultra, Operation*

*This page intentionally left blank*



## U-2 Incident

■ LARRY GILMAN

The U-2 spy plane, a high-altitude reconnaissance aircraft built by the U.S. starting in the 1950s, was the subject of many “incidents” or diplomatic confrontations with the Soviet Union during the Cold War; however, the debacle referred to as *the* U-2 incident began on May 1, 1960, when a U-2 plane flown by Central Intelligence Agency (CIA) pilot Gary Powers took off from a U.S. air base at Peshawar, Turkey. The mission scheduled for Powers, codenamed Grand Slam, was to be the most ambitious U-2 flight undertaken up to that time. Its route would take it from Turkey to Soviet nuclear-weapons facilities in the Ural Mountains, various railroads, intercontinental ballistic missile sites in Siberia, then back across northern Russia, there to photograph shipyards before leaving Soviet airspace above the Arctic Circle and landing in Bodo, Norway.

The mission was unsuccessful. Powers took off at 6:26 A.M. on what was to have been the twenty-fourth U-2 overflight of the Soviet Union. He flew first to the east, over Iran to Afghanistan, in order to cross the Soviet border from an unexpected direction. He was, however, detected by Soviet radar while still 15 miles from the Afghan-Soviet border. Although undesirable, detection was not unusual; in fact, all previous U-2 flights over the Soviet Union had been detected at some point. The U-2 relied for success not primarily on stealth but on the fact that the Soviets had no fighter planes or, for the first few years, surface-to-air missiles that could fly high enough (70,000 ft [21 km]) to shoot it down. A recently deployed Soviet surface-to-air missile, the SA-2, could reach the U-2, but only if it happened to be stationed in the plane’s flight-path and if its operators were on alert status, ready to fire.

Powers flew over an SA-2 battalion soon after entering Soviet airspace, but its crew was not on alert and so

could not fire while he was within range. About a dozen Soviet MiG fighter planes also attempted to shoot down Powers’s U-2, but could not climb high enough to get within weapons range.

Soviet premier Nikita Khrushchev (1894–1971) was notified of Powers’s ongoing flight at 8:00 A.M. Moscow time. It being May 1 (May Day or International Labor Day), he was preparing for the massive official festivities that always scheduled for that occasion. Outraged at what he perceived as a deliberate political provocation, he ordered that Powers’s U-2 be shot down at any cost.

By this time Powers was approaching the Russian city of Sverdlosk. The pilot of an Su-9 fighter jet was ordered to carry out a suicide attack on Powers, ramming the U-2 with his own plane; however, he was unable to locate Powers. An SA-2 battalion stationed outside the city was on alert, and when Powers entered its zone of engagement it fired a missile. It exploded near Powers’s plane. The fragile U-2 was damaged by the concussion and began to break to pieces. Powers managed to bail out, and was captured as soon as he parachuted to the ground.

Because the U-2 overflights violated treaty law, the U.S. always denied publicly that they were occurring. Early on, in fact, the CIA, which ran the U-2 program, had considered using non-U.S.-citizens as pilots. Therefore, after the loss of Powers’s plane (but before the Soviet Union had revealed that it had captured Powers alive) the U.S. issued several false cover stories. The National Aeronautics and Space Administration (NASA), for example, claimed that it had lost a U-2 being used as a weather plane over Turkey; the idea was that if the Soviets recovered the plane itself, the U.S. would claim that it had strayed accidentally into Soviet airspace when its oxygen supply failed and the pilot lost consciousness. A spokesman for the U.S. Department of State assured reporters at a press conference in Washington, D.C., on May 6 that “There was no—N-O—no deliberate attempt to violate Soviet air space, and there has never been,” and added that it was “monstrous” of the Soviets to assert that the U.S. would lie to the world.

But the next day, May 7, Khrushchev revealed that he had proof that the U-2 had been a spy plane: Powers himself. The statements by NASA and the State Department were exposed, causing an international political embarrassment for the U.S. On May 11, President Eisenhower made a speech in which he admitted that the U.S. had been overflying the Soviet Union. That same day, the remnants of Powers's U-2 were put on public display in Gorky Park in Moscow and were toured by Soviet leaders. Political protest in Japan caused the U.S. to withdraw its U-2 detachments from that country; soon the U.S. had withdrawn all its other overseas U-2 detachments as well. For the U.S., both the political and operational costs of the U-2 incident were high.

Powers was questioned, but revealed nothing of value to his captors. He was sentenced to 10 years in prison as a spy but was traded back to the U.S. for a captured Soviet spy two years later. Coincidentally, the day Powers was sentenced—August 19, 1960—the U.S. made its first use of a technology that would eliminate altogether the need for U-2 overflights of the Soviet Union, recovering a film package from its first spy satellite, the Corona. The Corona's pictures showed more of the Soviet Union (albeit at lower resolution) than all reconnaissance missions made up to that time by the U-2 and high-altitude balloons. From that day forward satellites, not airplanes, would provide direct intelligence of Soviet activity—and would do so without political risk.

## ■ FURTHER READING:

### BOOKS:

Peebles, Curtis. *Shadow Flights: America's Secret Air War against the Soviet Union*. Novato, CA: Presidio. 2000.

### SEE ALSO

*U-2 Spy Plane*

## U-2 Spy Plane

■ LARRY GILMAN

The U-2 is a jet-powered reconnaissance aircraft specially designed to fly at high altitudes (i.e., above 70,000 ft [21 km]). It was used during the late 1950s to overfly the Soviet Union, China, the Middle East, and Cuba; flights over the Soviet Union, the primary mission for which the plane was designed, ended in 1960 when a U-2 flown by CIA pilot Gary Powers was shot down over the Soviet Union. This event was a major political embarrassment for the U.S. A redesigned version of the U-2, the U-2R, was used from

the late 1960s through the 1990s. The U-2R was used extensively during the Gulf War of 1991, for example, to monitor Iraqi military activities. A more recent version of the U-2, the U-2S, is deployed today. The U-2S has been used recently by both the United States and United Nations weapons inspectors to make observations of North Korea and Iraq.

**Background.** Shortly after the end of World War II, the tenuous alliance between the Soviet Union, the United States, and the nations of Western Europe ruptured. The Soviets took control of Eastern Europe, the North Atlantic Treaty Organization (NATO) was formed by the U.S. and its European allies, and the Cold War began in earnest. Tensions were high, and war between NATO and the Soviet Union often seemed imminent. Military planners desired what they termed “pre-D-day intelligence” about the Soviet order of battle, that is, information about the Soviet military obtained before a war began. Spy satellites would not become available until the early 1960s, leaving aircraft as the primary means of obtaining up-to-date information about Soviet military and industrial activities.

A number of photographic spy overflights of Eastern Europe, the Soviet Far East, China, and the periphery of the Soviet Union were made in the late 1940s and early 1950s using various U.S. and British aircraft including the RB-29 bomber, the B-47B bomber, the RF-80A fighter (the first operational U.S. jet fighter), the RF-86F fighter, and the RB-45C reconnaissance aircraft. None of these planes had enough range to penetrate very far into Russia itself, where nuclear testing grounds and missile bases were located; nor could they fly at altitudes high enough to avoid interception by Soviet MiG jet fighters.

By the mid-1950s, Soviet air defenses had improved to the point where overflights by available aircraft had become impractical. Development of a lightweight, high-altitude, single-pilot plane (originally dubbed the CL-282 but later the U-2, a deliberately misleading designation suggesting a “utility” aircraft) began in 1954. However, the plane could not ready until 1956; in the meantime, high-altitude, unmanned balloons were used to carry camera packages over the Soviet Union. These balloons, codenamed Genetrix balloons, were launched in Norway, Scotland, Turkey, and West Germany, from whence they were carried by global tradewinds across the Soviet Union to recovery zones over the Pacific Ocean. Some 379 Genetrix balloons entered Soviet airspace in 1955 and 1956; 235 were shot down by MiGs or antiaircraft guns, and only 44 were recovered. The success rate would have been higher except that President Dwight Eisenhower had ordered that the balloons not fly at their true maximum altitude (70,000 ft [21 km]); he reasoned that if the balloons were restricted to an altitude ceiling of 55,000 ft (17 km), where the Soviets could shoot them down most of the time, the Soviets would not be motivated to develop high-altitude interceptors that could be later used against the U-2.



Gary Powers, shown while an Air Force Reserve pilot, later flew an American U-2 spy plane over Russia in 1960 and was shot down, held prisoner, was subjected to a public show-trial, and ultimately returned to the West in exchange for a Russian spy. AP/WIDE WORLD PHOTOS.

**Design.** The U-2 is built much like a glider, with ultralight construction and long, narrow wings that measure 80 ft (24 m) from tip to tip, longer than the plane itself. (The U-2C, first flown in 1978, has a wingspan of 103 ft [31 m].) Wings of this type, mounted at right angles to the body of an aircraft, provide high lift (i.e., upward aerodynamic force resulting from airflow around the wing); this is necessary at 70,000 ft because the atmosphere is so thin. The U-2's cruising altitude takes it so close to outer space that the sky above appears black and the curvature of the Earth is visible.

The U-2 had other features intended to reduce its weight and thus increase its cruising altitude and range. The wings were bolted to the body of the aircraft rather than supported, as in standard jet aircraft of that period, by a spar running right through the fuselage. The tail assembly was held on by only three bolts; the skin of the fuselage was thin aluminum; flight controls were manually powered, so the pilot flew the plane by muscle power; and there was no radar. In-line "bicycle"-type landing gear was employed, consisting of a main unit under the plane's nose and small wheel at the tail; upon landing, the U-2 would taxi to a halt and then tip over onto one wing. For takeoff, small detachable supports or "pogos" held the wings off the ground and were dropped when the plane was airborne.

A camera package termed the A-2 was installed in the aircraft's belly; it contained three still cameras, one pointing straight down and the other two pointing to the left and right of the aircraft's direction of travel, as well as a tracking camera that filmed a continuous record of the plane's mission.

Development of the U-2 and of reconnaissance balloons required numerous test flights over the United States. The balloons were often visible from the ground as metallic-looking ellipses, and prototype U-2 planes were sometimes spotted from civilian airliners; these sightings giving rise to many reports of unidentified flying objects (though to be alien spacecraft). Because the devices actually causing the sightings were secret, the government offered often uncredible explanations for the sightings, inadvertently helping to encourage bizarre UFO beliefs.

Because of the need to fly light, the U-2 does not carry weapons. Nor can it undertake evasive maneuvers if fired upon, for it is delicate, and breaks up if subjected to strong forces. It is designed to fly high and far.

**Deployment.** On June 20, 1956, the first U-2 flight over a "denied area"—Warsaw Pact airspace—was made. The flight passed over Czechoslovakia, Poland, and East Germany. On July 1956, flights over the Soviet Union itself commenced, with a flight over Leningrad to photograph the shipyards. MiG fighters attempted to intercept the U-2, which was detected by Soviet radars, but were unable to attain its altitude. The next day a U-2 overflew Moscow

itself, photographing the Kliningrad missile factory and Khimki rocket-engine factory north of the city.

Although the U.S. did not officially admit the existence of the U-2 flights, due to Soviet diplomatic protests President Eisenhower ordered all U-2 overflights of the Soviet Union temporarily suspended late in 1956. U-2s were used during this interval to spy on French and British actions in the Middle East during the Suez Crisis. Eisenhower ordered U-2 flights resumed after the Soviets crushed the Hungarian rebellion of October 1956. This Soviet aggression heightened tensions between NATO and the Warsaw Pact and increased the U.S. desire for intelligence data. Over the next few years, the U-2 was flown over China and Vietnam as well the Middle East, Eastern Europe, and the Soviet Union.

On May 1, 1960, a U-2 was shot down over Russia by a surface-to-air missile. The pilot was captured, tried for espionage, and sentenced to 10 years in prison. (He was traded for a captured Soviet spy two years later.) No more overflights of the Soviet Union were attempted. Coincidentally, however, the U.S. spy satellite program accomplished its first recovery of a film packet from space on the day that Powers was sentenced (August 19, 1960). The U-2 was, therefore, no longer a unique source of intelligence about affairs inside Soviet territory. However, it still had an important role to play in military history. On October 14, 1962, a U-2 flying over Cuba took pictures that proved that the Soviet Union had established sites for launching medium-range ballistic missiles in Cuba. The presence of these nuclear-armed missiles in Cuba, combined with U.S. insistence that they be removed, gave rise to the Cuban Missile Crisis, which almost resulted in war between the U.S. and Soviet Union in October 1962.

Despite radical improvements in spy satellite capabilities since the 1960s, U-2 planes continue to provide some intelligence data. Some experts believe that U-2S photographs of North Korean facilities were the basis of the U.S. discovery in October 2002 that North Korea was producing enriched uranium for nuclear weapons. In 2003, proposed U-2S overflights of Iraq to support United Nations weapons inspections were a subject of controversy between the U.S. and Iraq. Furthermore, a civilian version of the U-2, the ER-2, is used by the U.S. National Aeronautics and Space Administration for Earth-resources research. The ER-2 has even made flights over Russia—with official permission.

#### ■ FURTHER READING:

##### BOOKS:

Peebles, Curtis. *Shadow Flights: America's Secret Air War against the Soviet Union*. Novato, CA: Presidio, 2000.

##### SEE ALSO

*U-2 Incident*

## Ukraine, Intelligence and Security

Much of Ukraine's intelligence and special operations structure bears the imprint of the nation's Soviet past. Both the Security Service of Ukraine (Sluzhba Bespeky Ukrayiny; SBU) and its principal action unit are based on Soviet models. Internationally, the Ukraine has come under suspicion as a supplier of materials to rogue states and groups.

Founded in 1991, the SBU took over the old KGB Ukrainian headquarters in the capital city of Kiev. It also took on the organization structure, in many cases the tactics, and even many of the personnel of its Soviet predecessor. Like KGB, it oversees both security and intelligence operations, and through its subunit GUR, fights organized crime, terrorism, drug trafficking, and arms smuggling. Another important SBU subunit is the action group Administration A, the "Alpha" unit. Named and modeled after the Soviet Alpha unit that attacked the presidential palace in Kabul in 1979, setting off the Soviet-Afghan war, it has counterterrorism and witness protection responsibilities.

Despite its stated opposition to terrorism, Ukraine has been accused to supplying materiel to terrorist states and groups. Not only did it supply two helicopters to Slobodan Milosevic's Serbia in 1999, but in 2002, it was under investigation by United States and British arms experts on allegations that it had sold sophisticated Kolchuga radar systems to Iraq. Ukraine has also been accused, along with Russia and the regime of President Aleksandr Lukashenko in Belarus, of selling weapons to rebel armies in Sierra Leone and Liberia. Western intelligence sources also reported that representatives of Afghanistan's Taliban regime and the Muslim terrorist network al-Qaeda visited Kiev in September 1999, looking to purchase arms, parts, and training.

### ■ FURTHER READING:

#### BOOKS:

- Anderson, Robert. "The Former Soviet Republics Are Accused of Supplying Weapons to Rogue States in Defiance of United Nation or U.S. Embargoes." *Financial Times* (October 21, 2002): 27.
- Bennett, Richard M. *Espionage: An Encyclopedia of Spies and Secrets*. London: Virgin Books, 2002.
- Kuzio, Taras. "Details Emerge on Kiev's 'Alpha' Unit." *Jane's Intelligence Review* 11, no. 10 (October 1, 1999): 1.
- Warner, Tom. "U.S. Plans to Shun Ukraine President over Radar." *Financial Times* (November 9, 2002): 10.

#### ELECTRONIC:

Ukraine Intelligence. Federation of American Scientists. <<http://www.fas.org/irp/world/ukraine/>> (March 1, 2003).

### SEE ALSO

KGB (Komitet Gosudarstvennoi Bezopasnosti, *USSR Committee of State Security*)  
Russia, *Intelligence and Security*

## Ulster Defense Association/ Ulster Freedom Fighters (UDA/UUF)

The Ulster Defense Association/Ulster Freedom Fighters (UDA/UUF) is the largest loyalist paramilitary group in Northern Ireland, and was formed in 1971 as an umbrella organization for loyalist paramilitary groups. It remained a legal organization until 1992, when the British Government proscribed it. Among its members are Johnny Adair, the only person ever convicted of directing terrorism in Northern Ireland, and Michael Stone, who killed three people in a gun and grenade attack at an IRA funeral. The UDA joined the UUF in declaring a cease-fire in 1994, which broke down in January 1998, but was later restored. In October 2001, the British Government ruled that the UDA had broken its cease-fire. The organization's political wing, the Ulster Democratic Party, was dissolved in November 2001. The group has been linked to pipe bombings and sporadic assaults on Catholics in Northern Ireland; where it stepped up attacks in 2001. William Stobie, the group's former quartermaster who admitted to passing information about the UDA to the British government, was murdered in December 2001; the Red Hand Defenders claimed responsibility for the killing.

Estimates of UDA strength vary from 2,000 to 5,000 members, with several hundred active in paramilitary operations throughout Northern Ireland.

### ■ FURTHER READING:

#### ELECTRONIC:

- CDI (Center for Defense Information), Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <<http://www.cdi.org/terrorism/terrorist.cfm>> (April 17, 2003).
- Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).
- Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001," Annual Report: On the Record Briefing. May 21, 2002 <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).
- U.S. Department of State. Annual Reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).



## SEE ALSO

*Terrorism, Philosophical and Ideological Origins*  
*Terrorist and Para-State Organizations*  
*Terrorist Organization List, United States*  
*Terrorist Organizations, Freezing of Assets*

---

## Ultra, Operation

---

■ ADRIENNE WILMOTH LERNER

Operation Ultra was the codename for the British cryptologists efforts at Bletchley Park to intercept and break German coded messages. While Ultra initially was the cryptonym for the project to break the German Enigma machine, the code name came to represent all British efforts to break high-level German radio codes during World War II.

### Bletchley Park and Operation Ultra

Surveillance of high-level German communications began at Bletchley Park in 1938. Thirty code breakers, linguists, mathematicians and other experts formed the first class of the new government cipher school. Within a year, British military intelligence employed over 500 people at Bletchley Park. The cryptology team had several early successes breaking lower-level German government intercepts that used mathematical and word replacement codes. However, a complex, machine-produced mathematical cipher, appeared in the wire traffic. British codebreakers nicknamed the foreign cipher machine Enigma. As tensions in Europe escalated, and war seemed imminent, Enigma intercepts increased from a few to a few hundred a day. In 1939, Operation Ultra charged cryptologists with breaking the Enigma code and devising a rapid means of transcribing the intercepts.

The breaking of Enigma began even before the creation of the Bletchley Park cryptanalysis department. Polish intelligence began monitoring German communications and breaking their codes in the mid-1930s. However, the Germans created a new cipher, Enigma, in the summer of 1938. When Britain and France pledged their support to ensure Poland's freedom from invasion and domination by Nazi Germany, Polish intelligence shared all of their code-breaking information and technology with Britain and France. Defying the Munich Agreement, Germany invaded Poland in 1939, beginning World War II.

British cryptologists decoded German communications with limited success in the early months of the war. Some codes were broken mathematically and then decoded in long hand, an arduous process. Other codes,

mainly used for low-level security communications used decades-old codes broken by French, British, Polish, or Swedish intelligence. In 1940, mathematicians at Bletchley Park broke the German Enigma machine. Modifying plans given to them by the Poles, Ultra engineers constructed a bombe, a code-breaking machine, to aid in deciphering Enigma intercepts. Naval WRENs, members of the Royal Navy women's corps, operated the noisy, large, and cumbersome bombes. Throughout the war, women on staff at Bletchley Park outnumbered men eight to one.

Gathering coded data and intercepting German messages was almost as grueling a task as deciphering the communications. British military signals and radio specialists staffed thousands of "Y" intercept stations on the coast and in Europe. Transmissions were affected by weather phenomena, interference from jamming machines, background noise, and congested airwaves. Thus, intercepted data was often difficult to understand. The German government and military used over 200 frequencies to broadcast messages, most of which lasted less than 30 seconds. Coded wire traffic was often broken off in mid course or sent over new. Wires known to be tapped were constantly replaced. What communications data was collected at the stations was then sent to Bletchley Park cryptologists and translators, either by courier or coded teleprinter.

Ultra staff and technology successfully decoded over 50 messages a week. However, by 1942, German radio and wire traffic increased exponentially. The 1,200 member staff of Bletchley Park could not efficiently decipher the thousands of intercepts received daily. Even the construction of more bombes did not significantly aid progress on Ultra. Since the decoding, translating, and transcription process was slow, the intelligence gathered from intercepts could not be used to its full potential. When British cryptologists broke the more complicated German *Geheimschreiber* cipher machine, Ultra intelligence nearly doubled.

Engineers Alan Turing and Tommy Flowers devised a complex machine to decipher and transcribe German intercepts. The device, appropriately nicknamed Colossus, could handle the thousands of intercepts arriving daily at Bletchley Park. The massive task of transcribing and photographing decoded messages for storage in the archives was greatly reduced since Colossus transcribed the messages, in the original German, directly on to a typewriter. Colossus proved so efficient that British intelligence soon learned it could decipher messages more rapidly than could the intended recipients. Ultra intelligence became a key part of British battle strategy, giving British military command advance information on German military operations.

**Secrecy and security.** Worried that the German military and government would change encryption devices if they knew

of the operation, Ultra was shrouded in absolute secrecy. For security, the details of the entire Operation Ultra were fully known by only four people, only one of whom routinely worked at Bletchley Park. Dissemination of Ultra information did not follow usual intelligence protocol, but maintained its own communications channels. Military intelligence officers gave intercepts to Ultra liaisons, who in turn forwarded to the intercepts to Bletchley Park. Information from decoded messages was then passed back to military leaders through the same channels. Thus, each link in the communications chain knew only one particular job, and not the overall details of Ultra.

The massive archives of intercepts decoded at Bletchley Park were reproduced in entirety. A photograph of each intercept, and its English translation, were archived at the Bodleian Library at Oxford University in case German forces located and bombed the Bletchley Park complex. A train was on constant reserve at nearby Bletchley Station to ferry code breaking records and equipment to Liverpool, from where it would be shipped to American intelligence headquarters in the event of a German invasion.

Within Britain, the Ultra secret was closely guarded. However, British intelligence did share cryptological advances, including information on Ultra and the Enigma machine, with the American and French intelligence community. Joint American-British information exchanges became more commonplace. American intelligence shared information on Magic, their code-breaking operation against Japan. In the months before Pearl Harbor, a group of American cryptologists was sent to Bletchley Park to observe British code-breaking operations. Information provided by Bletchley Park aided American cryptologists in breaking the Japanese Purple machine. Germany shared their encryption technology with its Japanese allies. As was the case with Enigma, Allied cryptologists broke the Purple machine but the Japanese continued to use its code throughout the war. American code-breakers also worked on German codes and the design of decoding machines. The American department working on German codes also called itself Ultra.

While the British shared details of Ultra with American and French intelligence, the project was kept secret from the Soviet Union, despite the Soviets' status as wartime allies. Soviet intelligence knew of Bletchley Park, but the British kept the fact that cryptologists broke the Enigma code secret. Information from important messages containing German battle plans and troop positions was disguised as intelligence gathered from Resistance groups in France and Switzerland. Soviet military intelligence believed the information originated from operatives in the Communist spy network, Sandor Rado.

**Ultra intelligence and the Allied war effort.** Operation Ultra's major shortcoming was that intelligence dispatches were not processed quickly enough in the early war years to aid in the Battle of Britain, and spare London the full force of

the Blitz. German U-boats dominated the seas, and Allied fighter commands had little reliable intelligence information until 1942.

With the invention of Colossus, a secure and reliable network through which to disseminate information, and the tireless work of the Bletchley Park staff, Ultra information was successfully used in several pivotal Allied military operations. Monitoring German naval dispatches, code-breakers determined fleet positions, allowing convoys to divert their routes and safely cross the Atlantic. German U-boats lost their strategic element of surprise, and Allied forces located and sank the German submarines with increasing frequency. One of the great victories and British morale boosters during the war was the sinking of the German destroyer *The Bismarck*.

While the guarantee of safe passage for Allied supply ships was important in the Atlantic, it was vital in the smaller waters of the Mediterranean Sea. Ultra intercepts noted that the Germans anticipated an assault on Sicily. Allied forces postponed their invasion until they convinced German forces they intended to invade the Balkans and Greece. False communications sent via a British-built Enigma machine added to the ruse, and the German army redeployed troops to the Balkans. Ultra intercepts confirmed the revised German troop positions, and the Allies then continued with their planned invasion of Sicily and Italy.

Ultra information regarding Hitler's "Atlantic Wall" defenses in France helped Allied forces plan the D-Day invasion. Ultra intercepts yielded information that German high command thought that an Allied invasion of France, if it occurred, would most likely take place on the beaches near Pas de Calais. The British planted false information for German intelligence, the *Abwehr*, to confirm their suspicions. The Germans diverted a significant number of troops to the area, lessening the defenses on the northern Normandy beaches where the Allied invasion landed. As Allied troops progressed through France, commanding officers received daily Ultra intelligence updates.

The closely guarded secret of Ultra was never discovered by the Axis powers. Germany continued to use Enigma throughout the war, giving the Allies a decided tactical advantage and nearly eliminating the element of surprise in German offensives. After the war, the cryptology department at Bletchley Park was disassembled, the archives removed to classified storage, and the complex deciphering equipment destroyed. The veil of secrecy extended to the wartime staff of Bletchley Park, none of whom disclosed information about Ultra until the project was officially declassified in 1989. Bletchley Park secrets were so closely guarded that one of the major accomplishments of Operation Ultra was slighted its deserved historical recognition. The electronic, programmable Colossus, with its 2,500 tubes, predated the American ENIAC machine, widely regarded as the world's first computer, by two years.

■ FURTHER READING:

BOOKS:

- Hinsley, F. H. *British Intelligence in the Second World War*. Cambridge: Cambridge University Press, 1988.
- Hinsley, F. H. and Alan Stripp, eds. *Codebreakers: The Inside Story of Bletchley Park*. Oxford: Oxford University Press, 2001.
- Stinson, Douglas. *Cryptography: Theory and Practice*, second edition. Chapman and Hall, 2002.

SEE ALSO

- Bombe*  
*Codes and Ciphers*  
*Codes, Fast and Scalable Scientific Computation*  
*Colossus I*  
*FISH (German Geheimschreiber Cipher Machine)*  
*Operation Magic*  
*Purple Machine*  
*World War II, United States Breaking of Japanese Naval Codes*

Ultrashort-Pulse Laser Technology.

SEE *Lawrence Livermore National Laboratory (LLNL)*.

Underground Facilities,  
 Geologic and Structural  
 Considerations in  
 the Construction

■ WILLIAM C. HANEBERG

Natural and manmade underground facilities have played an important role in warfare and national security for more than 5000 years. Underground chambers were used for hiding places and escape routes in Mesopotamia and Egypt from 3500 to 3000 B.C., and they continue to play an important role in the ongoing conflict in Afghanistan. Some notable twentieth-century uses of underground facilities for warfare and national security include dozens of underground factories constructed beneath Germany during World War II; the Cheyenne Mountain Operations Center, Colorado; as many as 1000 underground facilities estimated to exist beneath the Korean Demilitarized Zone; and countless natural and manmade caves used by al-Qaeda forces in Afghanistan. Large manmade cavities in salt domes along the Gulf Coast, some of them larger than 17 million cubic meters in volume, are used for the United

States Strategic Petroleum Reserve. The details of underground facilities used for military or national security purposes are classified, but there is no reason to assume that they are not on the scale of underground civil projects. The largest unsupported span ever constructed in rock was a 61 m (200 ft) wide hockey arena constructed for the 1994 Winter Olympics in Norway, and underground mines in many parts of the world consist of smaller passages that extend for many miles.

Extensive underground facilities have also been constructed to maintain communications and house the United States government in the event of an attack. An underground facility known as Site R exists within Raven Mountain, Pennsylvania, and is thought to have been the location from which Vice President Cheney and other officials worked in the aftermath of the September 11, 2001 terrorist attacks. Construction of Site R was authorized by President Truman and completed during the early 1950s. Declassified information dating from the construction period describes a three-story underground facility with more than 18,000 square meters of floor space and room for more than 5000 people. The existence of another extensive underground facility beneath the Greenbrier Resort in West Virginia, constructed to house the United States Congress in the event of a nuclear attack, was made public in 1992.

Although they can be expensive and difficult to construct, underground facilities offer two important advantages over surface structures. First, they are almost completely hidden from view and activities within them can be invisible to even the most sophisticated intelligence satellites. Second, their depth can make them resistant to conventional and some nuclear attacks. Additional advantages include lower long-term maintenance costs (because underground structures are not exposed to weather) and lower heating and cooling costs (because temperature is constant in underground environments). The detection and characterization of underground facilities and the development of technologies to defeat hardened underground facilities are among the principal goals of modern military geologists.

Geologic factors exert an important influence on the design and construction of any underground facility. One of the most important factors is the strength of the soil or rock into which underground structures are excavated. Shallow underground structures can be constructed in soil or highly weathered rock using a technique known as cut-and-cover construction. These structures are built by first excavating a hole, then building the desired facilities, and finally covering the completed structures with soil. Because soil and weathered rock near Earth's surface tends to be weak, shallow cut-and-cover structures must be heavily reinforced with concrete or other materials if they are to withstand attack. The mineral quartz, which can be a common component of the rocks that are used for concrete aggregate, changes volume when it undergoes a phase transition at high temperatures (844 degrees K at a



A car enters the U1a Complex, an underground facility in Nevada designed for conducting subcritical experiments to determine whether aging nuclear weapons remain reliable and safe. AP/WIDE WORLD PHOTOS.

pressure of 0.1 MPa). In order to prevent thermal disintegration, therefore, aggregate for concrete that may be subjected to extremely high temperatures must consist of rocks containing little quartz. Cut-and-cover structures can be difficult to hide during construction, when they can be easily pinpointed on remote sensing images or aerial photographs. It may also be possible to locate shallow cut-and-cover structures after construction if soil disruption or activity within the structure produces a thermal, soil moisture, or soil chemistry anomaly identifiable through multispectral or hyperspectral image analysis.

Deep underground facilities can be constructed using specialized tunnel boring machines (TBMs) or by underground drilling and blasting. These construction techniques are used extensively in the underground mining industry and the construction of civil works such as tunnels. Tunnel boring machines are large pieces of construction equipment with faces that consist of rotating cutting tools, allowing the machine to drill itself into earth or rock and create tunnels many meters in diameter. Underground construction by drilling and blasting begins with a carefully designed pattern of holes drilled into a rock face. The holes are loaded with explosive charges that are detonated according to a specified sequence in order to efficiently fracture and loosen the rock, which is then removed to expand the underground opening.

The primary geologic factor controlling underground construction in rock is the nature of the rock itself. Strong rock with uniform physical properties is the preferred choice for underground construction. Clandestine tunnels excavated beneath the Korean Demilitarized zone by North Korea, for example, tend to be located in granite that is

relatively uniform and contains few fractures rather than adjacent rocks that are more highly fractured. Depending on the geologic setting of an underground facility, selecting choice rock may not be an option. Rocks are commonly heterogeneous, with physical properties such as strength and degree of natural fracturing varying from place to place.

Engineering geologists and civil engineers commonly describe the physical quality of rock using a simple parameter known as the Rock Quality Designation, or RQD, which is obtained by measuring core samples obtained during exploratory drilling prior to construction. The RQD is the percentage of pieces of core sample longer than 10 cm (4 in) divided by the total length of core. Thus, a core sample of intact rock with no fractures or cracks would have an RQD of 100. A core sample of highly fractured rock in which only one-quarter of the pieces are longer than 10 cm would have an RQD of 25. Other factors that affect the design and construction of underground facilities in rock include the number and density of natural fractures in the rock, the roughness of fracture surfaces and the degree of natural chemical alteration along fracture surfaces (both of which affect rock strength), the presence or absence of water in the fractures, and the presence or absence of zones of weakness such as faults or rock that has been altered to the consistency of clay. Highly fractured rock near a large fault, for example, may be too weak to support itself above an underground cavity or serve as a conduit for high-pressure water that can quickly flood an underground opening. Completion of the NORAD underground facility in Cheyenne Mountain during the 1960s, for example, was delayed for more than a year because of problems with a geologic fault intersecting the ceiling of the

underground opening. Underground openings in weak, highly fractured, or water saturated rock can be lined with reinforced concrete or shored with steel beams in order to ensure the safety of construction workers and later occupants of the space. The lithostatic stress that must be resisted by underground openings of any size increases linearly with depth, and the most stable underground openings are generally circular or spherical. Rectangular or cubic openings contain sharp corners that concentrate stresses in the rock and can lead to the collapse of the opening.

One issue that is important for military or security-related underground facilities, but generally not for civil structures, is their vulnerability to attack by conventional or nuclear weapons. The vulnerability of an underground facility to a conventional weapon attack is a function of its depth, the strength of the overlying rock, and the penetrability of the soil or rock exposed on Earth's surface above the facility. Knowledge of these properties is essential to those designing facilities to survive attacks as well as to those designing specialized earth penetrating weapons (EPWs). The geologic information necessary to evaluate the vulnerability of a facility has been given the name "strategic geologic intelligence" by some military geologists. Few, if any, underground facilities can withstand a direct nuclear attack.

#### ■ FURTHER READING:

##### BOOKS:

Underwood, J. R., Jr. and P. L. Guth, editors. *Military Geology in War and Peace*. Boulder, Colorado: Geological Society of America, 1998.

##### PERIODICALS:

Weiser, Carl. "'Secret' Government Site Not So Secret after All." *USA Today* (June 26, 2002).

##### ELECTRONIC:

Leith, William. "Military Geology in a Changing World." *Geotimes*, American Geological Institute. February 2002. <[http://www.agiweb.org/geotimes/feb02/feature\\_military.html](http://www.agiweb.org/geotimes/feb02/feature_military.html)>(December 10 2002).

Linger, D.A., G.H. Baker, and R.G. Little. "Applications of Underground Structures for the Physical Protection of Critical Infrastructure." *CE World*. 2002. <<http://www.ceworld.org/ceworld/Presentations/CriticalInfrastructure/Applications-of-Underground-Structures-for-the.cfm>> (December 11 2002).

"Rock Tunnelling Quality Index." Edumine. <<http://www.edumine.com/Xtoolkit/tables/rtqitable.htm>>(December 11 2002).

U.S. Air Force. "Cheyenne Mountain Operations Center." <<https://www.cheyennemountain.af.mil/cmocindex.html>>(December 11 2002).

#### SEE ALSO

*Architecture and Structural Security*

*Continuity of Government, United States  
Geologic and Topographical Influences on Military and  
Intelligence Operations  
Hardening  
Vulnerability Assessments*

## Undersea Espionage: Nuclear vs. Fast Attack Subs

■ JUDSON KNIGHT

In developing its submarines, the United States has tended to pursue technical, rather than numerical, superiority. Such was the case during the Cold War, when the United States led in nuclear submarine development while the Soviets marshaled a much larger submarine fleet. After the Cold War concluded, Washington was faced with the possible threat of non-nuclear submarine deployment by third world nations.

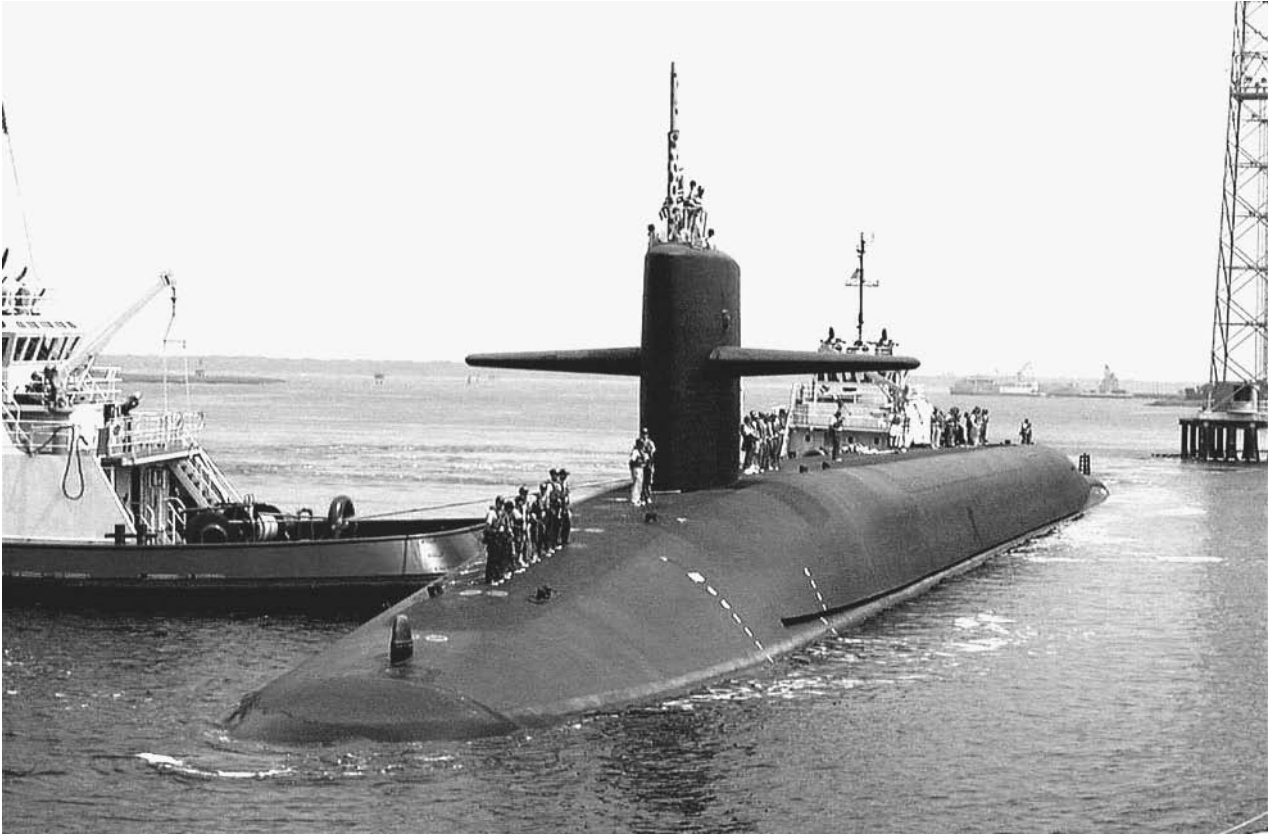
### U.S. Submarines

During the Cold War, there were two principal types of U.S. submarines, the fast attack submarine (SSN) and the nuclear-powered ballistic missile submarine (SSBN), nicknamed the "boomer." Both were nuclear-powered.

Fast attack submarines were tasked toward locating and tracking their Soviet counterparts, for which they carried extensive intelligence-gathering equipment. Their principal weapon was the torpedo, although at times they were armed with tactical missiles such as the cruise missile. The U.S. Navy's first nuclear sub was the *Nautilus*, commissioned on September 30, 1954. It was followed during the 1950s by almost two dozen other craft, including several in the Skate, Shipjack, and Triton classes.

**Sturgeon and Los Angeles classes.** The Navy inaugurated a new era with the commissioning of the *Sturgeon* on March 3, 1967. First in a 37-member class, the *Sturgeon* was powered by a single Westinghouse Model 5 pressurized-water nuclear reactor. Its speed was an impressive 20 knots (37 kph) on the surface and 25 knots (46 kph) when submerged. (These figures are approximate, since the exact speed of the *Sturgeon* class is classified.)

Another phase in this second generation of SSNs was the Los Angeles class, a group of 62 craft that can submerge to depths of 800 feet (240 m) or more. At 362 feet (110 m) long and 33 feet (10 m) abeam, they can accommodate a crew of 127 or more. The Los Angeles class was



The USS *Louisiana*, an Ohio-class nuclear powered submarine with an armament including 24 Trident II missiles, arrives at its home port in King's Bay, Georgia. AP/WIDE WORLD PHOTOS.

built during a period from the mid-1970s to the mid-1990s, and many are still in use.

**“Boomers” and beyond.** During the period from 1960 to 1966, the Navy introduced a total of 41 SSBNs, or “boomers.” This group was nicknamed “41 for Freedom,” because each was named after a hero from American history, as reflected in the names of the three classes: George Washington, Ethan Allen, and Benjamin Franklin. (The first two groups consisted of five submarines each, with 31 in the third group.) Each of these carried 16 Polaris nuclear missiles, but in 1972, conversion to the more accurate Poseidon missile began. By 1979, the even more advanced Trident I missile had been introduced, and the last 12 of the original 41 SSBNs were converted for this missile.

The next generation of SSBN arrived with the *Ohio*, which inaugurated a much larger class of sub in 1981. Ohio class subs are 560 feet (170.7 m) long and 42 feet (12.8 m) abeam. The first 12 were equipped to carry 24 Trident I missiles, and with the introduction of the Trident II in 1990, subsequent models were built for this newer, larger missile. The 18 SSBNs of the Ohio class together carry 50% of all U.S. strategic warheads.

Four of the Ohio class were scheduled for inactivation in 2003 and 2004, but instead they are being converted to guided missile submarines (SSGN). The primary mission of the latter will be support for land attack and special operations forces, a change that reflects that differences between the Cold War battlefield and more modern asymmetric warfare. SSGNs will be equipped with as many as 154 Tomahawk missiles.

## Soviet Submarines

In submarines as in much else, the Soviets lagged behind their Western foes, and what they lacked in sophistication and accuracy they attempted to make up for in numbers. Their first subs were based on German models observed during World War II. By the late 1950s, they had deployed their first diesel and electric ballistic missile submarines, and in 1960 launched their first nuclear-powered subs. The Soviets, with their more limited budgets, were actually decades ahead of the Americans in one area: the SSGN, which they first began operating in the 1960s.

By 1980, the Soviet Union had 480 submarines, of which 71 were fast-attack craft and 94 SSBNs or SSGNs. Among these was the Alfa class, built in the 1970s, which

had 30-man crews and could achieve speeds of 43 knots (80 kph) and depths of 2,000 feet (600 m). The Typhoon class, first deployed in 1977, was the largest class of submarines ever built, at a length of 563 feet (172 m) and a beam of 81 feet (25 m). The Soviets, unlike the Americans, continued to build diesel-electric subs. Among these were the Kilo class, which first entered service in 1979 and are still being built for export.

## Third World Submarines

From the early 1990s, it became apparent that the United States faced new challenges in the form of third-world nations armed with nuclear subs. Among these was Iran, which in 1993 deployed its first Kilo class subs in the Persian Gulf. Thus armed, the Teheran regime could close the Strait of Hormuz, through which one-quarter of the world's oil passes. Of the third-world countries that together possessed a total of 150 submarines, the largest share belonged to North Korea, with 25. Libya had six, as did Pakistan, whereas Pakistan's longtime foe India had 18.

Among the factors driving the sales to third-world countries was the collapse of the former Soviet Union, which had left Russia economically distressed and in need of hard currency. Given the fact that defense technology was one of the few areas in which the Soviet state had excelled, sales of submarines seemed a logical choice. Other, more prosperous Western European countries were also selling submarines to third-world countries, with Germany and France in the lead. At the same time, segments of the U.S. defense industry, facing downturns in production following the end of the Cold War, had begun to pressure Washington for an opportunity to gain a share of the emerging new markets in countries such as Egypt, Taiwan, and Argentina.

### ■ FURTHER READING:

#### PERIODICALS:

- Ahrens, Frank. "Submarines, Examined at Depth: The Smithsonian's New Nautical Exhibit Settles in for a Three-Year Tour." *Washington Post*. (May 8, 2000): C1.
- Arney, Kevin. "Midshipman Cruises Aboard Fast Attack Submarine." *The Officer* 73, no. 11 (November 1997): 57.
- Lehman, John. "Silent, Deep, Deadly." *Wall Street Journal*. (November 11, 1998): 1.
- Revelle, Daniel J., and Lora Lumpe. "Third World Submarines." *Scientific American*. (August 1994): 16–21.

#### ELECTRONIC:

- Navy Fact File: Attack Submarines. U.S. Navy Office of Information. <<http://www.chinfo.navy.mil/navpalib/factfile/ships/ship-ssn.html>> (April 7, 2003).
- Submarine Weapons. Smithsonian National Museum of American History. <<http://americanhistory.si.edu/subs/weapons/index.html>> (April 7, 2003).

### SEE ALSO

*Aircraft Carrier*  
*Cruise Missile*  
*P-3 Orion Anti-Submarine Maritime Reconnaissance Aircraft*  
*USSTRATCOM (United States Strategic Command)*

## Unexploded Ordnance and Mines

### ■ MIKE LAMBERT

Munitions (devices equipped with explosives or other material for use in military operations) can represent a hazard to people and to any future use of the land where they are located. As either the accidental or deliberate remnants of military activity, they represent a growing humanitarian and environmental problem in many parts of the world. There are two general categories of these munitions. The first, unexploded ordnance (often abbreviated "UXO") can be defined as munitions that are left in place due to either not detonating as intended, or by deliberate abandonment once military operations have ceased. The second, mines, are a type of unexploded ordnance that are deliberately hidden and which are meant to cause damage to people or property at a later time.

## Unexploded Ordnance

Unexploded ordnance is generally considered less dangerous than a mine because it is often found on the surface of the ground, although in many instances, unexploded ordnance can be feet or meters beneath the surface. Unexploded ordnance poses a potential hazard wherever it is found. Adults may attempt to collect unexploded ordnance as souvenirs or for resale as scrap metal. Children are at greater risk than adults because they are often attracted by the unusual objects and are unaware of the danger.

**Types and occurrence of unexploded ordnance.** The term ordnance refers to any munition, whether a bomb, bullet, grenade, or shell (or, strictly speaking, a mine) that contains an explosive device. Projectiles are ordnance that move and that can apply force through their own movement or inertia. The warhead of a projectile, containing the part of the munition intended to cause damage, can be a single unit or may be designed to fragment in operation. Bomblets are submunitions that are deployed separately from a parent munition, and a cluster bomb contains and disperses bomblets or submunitions. Cluster bombs were



In an effort to raise world attention about the dangers of unexploded land mines, Diana, Princess of Wales, watches a land-mine clearing demonstration in Huambo, central Angola, in 1997. AP/WIDE WORLD PHOTOS.

first deployed in the Vietnam War, and represent a growing source of danger from unexploded ordnance as they are used in more areas of combat.

When found on the sites of former ordnance supply depots, unexploded ordnance may be on the surface of the ground or just beneath the surface. At former bombing, artillery, or gunnery ranges, unexploded ordnance may be found at depths of several meters or feet if a projectile impacted the earth with considerable force and failed to detonate. The number of unexploded ordnance per acre depends on the size and intensity of use of a particular site. For example, the former Lowry Bombing Range in Colorado could have anywhere from 0.4 to 32 items of unexploded ordnance per acre, depending upon which organization is calculating the estimate (the smaller number comes from the U.S. Department of Defense, and the larger number is from the State of Colorado). On the other hand, the smaller but more intensively used former Southwest Proving Ground in Arkansas is estimated to contain 800 items of unexploded ordnance per acre.

**Unexploded ordnance clearance program.** The United States has made a systematic effort to clean up unexploded ordnance at former ordnance supply depots and military ranges. As recently as 1999, it was estimated that as many

as 2,657 former military sites needed to be cleared of unexploded ordnance in the U.S., and by 2002, that number was raised to 9,000. The Defense Environmental Restoration Program (for) Formerly Used Defense Sites gives the U.S. Army Corps of Engineers the task of environmental restoration (including the cleanup of unexploded ordnance) at all former defense sites, regardless of which branch of the service was originally responsible for operating the site. The Corps follows a program of investigation and restoration that is specific to the needs of each site. This may include clearance of unexploded ordnance at the surface or to a specified depth. The actual detection of unexploded ordnance uses many of the same techniques used in mine clearance (discussed below). At the end of the restoration activity, the site may be approved for unrestricted future use, or may have its possible future uses restricted so as to limit exposure of people to the site. Also, long-term monitoring of the site may be instituted to insure that any unexploded ordnance missed by the restoration activity is not brought to the surface by erosion or the freeze-thaw cycle.

## Mines

Mines, also called land mines, are a type of unexploded ordnance that will still function as originally intended. Usually carefully hidden in the shallow subsurface, they remain in place in order to explode in proximity to or in contact with a person or target. Because they can remain functional long after the end of the particular conflict in which they were deployed, mines create a lingering danger for anyone who comes near them. Originally developed for use in the American Civil War of the 1860s (where they were called torpedoes), mines from conflicts as long ago as World War I to as recent as the Balkan Wars of the 1990s are still causing injury today.

Mines come in a variety of designs, and new types of mines are constantly being developed to fill either an anti-personnel (death or injury of people) or anti-material (destruction or damage of equipment) function. They may be hidden individually, or in large numbers as a minefield so as to deny a potential adversary (or the local indigenous population) the use of a particular area. It has been estimated that as many as 60 people a day are killed by anti-personnel mines.

The United Nations has been involved in mine action (all aspects of mine education, detection, and removal) since it began working with the problem in Afghanistan in 1988. It acts primarily through the U.N. Department of Peacekeeping Operations, although eleven different departments or agencies within the U.N. are involved in some way with mine action. UNICEF (the United Nations Children's Fund) has been named the U. N. Focal Point for mine awareness education, and has published the U.N.'s International Guidelines for Landmine and Unexploded Ordnance Awareness Education. The International Committee of the Red Cross has its own mine/UXO awareness



programs that inform and work with affected communities that have mine problems. Humanitarian mine clearance is the removal of mines or unexploded ordnance under the auspices of a private humanitarian organizations (sometimes referred to as Non-Governmental Organizations, or NGOs), so as to allow the land to be used by the local community. One recent source lists 16 different such private organizations that are directly involved with mine and unexploded ordnance eradication, and eight other private organizations that work with communities affected by mines and unexploded ordnance.

Mine clearance (also called demining) has been described as consisting of two levels of activity. In the first level, which could be carried concurrently with a mine awareness program, an assessment is made of the scope of the problem through interviews and questionnaires given to the local population that is most directly affected by the presence of mines. The second level includes the location and removal of the mines. This may be done by a technique as simple as probing the ground with long sticks at regular intervals, exposing any solid objects that are encountered, and then removing any of the objects that turn out to be mines. Or, specially trained dogs may be employed to sniff out and indicate the location of explosives in the ground, followed by digging to reveal any mines and the subsequent removal of the mines.

Sophisticated electronic or geophysical methods have become widely used in the detection of both mines and other unexploded ordnance, and are utilized by demining technicians carrying detection equipment over the area to be examined for mines. These methods include electromagnetic induction (EMI), where an electrical current is induced and detected in buried metallic objects such as mine casings, and magnetometry that detects the distortions in the Earth's magnetic fields caused by buried ferrous objects. Conductive soils, interference from buried pipelines and artifacts, magnetic minerals, and plastic mine casings may cause difficulties in using these detection techniques. Ground penetrating radar (GPR) is not affected by these considerations, and instead reveals shapes of objects in the subsurface that might be mines. GPR is not considered to be as reliable as EMI or magnetometry, and the radar signal can be absorbed by vegetation or moisture in the soil. Newer technologies for use in mine detection include infrared (heat) imaging that detects the difference between how a buried mine and the surrounding soil retain or release heat. Vegetation interferes with this technique, and heat imaging can only detect mines within centimeters (inches) of the surface. Thermal neutron activation, already in use at some airports for detecting explosives in luggage, has also been proposed for the detection of explosives in buried mines. This would detect the high nitrogen content of explosives by bombarding the ground with neutrons and then looking for the specific gamma ray response of nitrogen. Problems with this technique include the need for a radioactive isotope as a source of gamma rays in the field.

In most cases, physical removal of mines in an area is still undertaken manually by technicians in the field, which is slow, labor-intensive, and dangerous. There are many mechanical systems for use in automated demining, such as large flail machines and milling machines, and proposed devices utilizing jets of water or lasers, but these have been criticized for their cumbersome nature and expense, the need for extensive logistical support, and the need to manually recheck areas where the machines have operated.

An international treaty to ban anti-personnel mines was signed by 122 nations in Ottawa, the capital of Canada, in December 1997. Formally entitled the Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-personnel Mines and on Their Destruction, and less formally known as the Ottawa Convention, this treaty was ratified by 132 nations as of 2003. The United States is one of 62 nations that has not ratified the treaty.

#### ■ FURTHER READING:

##### BOOKS:

- Bryden, A., and A. McAslan. *Mine Action Equipment: Study of Global Operational Needs*. Geneva, Switzerland: Geneva International Centre for Humanitarian Demining, 2002.
- Croll, M. *The History of Landmines*. Barnsley, South Yorkshire, Great Britain: Leo Cooper, 1998.
- King, Colin, ed. *Jane's Mines and Mine Clearance*. Coulsdon, Surrey, Great Britain: Jane's Information Group, 1998.
- McGrath, R. *Landmines and Unexploded Ordnance: A Resource Book*. Sterling, Virginia: Pluto Press, 2000.
- United States Environmental Protection Agency. *Interim Final Handbook on the Management of Ordnance and Explosives at Closed, Transferred, and Transferring Range*. Washington, D. C.: U.S. EPA Office of Solid Waste and Emergency Response, 2002.

##### PERIODICALS:

- Loeb, V. "Unexploded Arms Require Big Cleanup at 16,000 U.S. Sites." *Washington Post*. November 25, 2002.
- Sahlin, C., Jr. National Defense University Institute for National Strategic Studies, Washington, D.C. "Global Mine Clearance: An Achievable Goal?" *Strategic Forum* Number 43, 1998.

##### ELECTRONIC:

- Lambert, M. "Unexploded Ordnance: a Reference Guide for the Citizen." Environmental Science and Technology Briefs for Citizens. 2001. <<http://www.engg.ksu.edu/HSRC/Tosc/uxo.pdf>> (April 25, 2003).
- Canada Department of Foreign Affairs. "The Ottawa Convention Status Report." SAFELANE. April 2, 2003. <<http://www.mines.gc.ca/convention-en.asp>> (April 27, 2003).
- UNICEF. "International Guidelines for Landmine and Unexploded Ordnance Awareness Education." United

Nations. 2002. <<http://www.unicef.org/landguide/mineawar.pdf>>(April 24, 2003).

## United Kingdom, Counter-Terrorism Policy

■ TIMOTHY G. BORDEN

Prior to the September 11, 2001, terrorist attacks on the United States, counter-terrorism programs in the United Kingdom focused mainly on the Irish Republican Army (IRA), a militant group committed to ending British control of Northern Ireland. After the bombing of Pan Am Flight 103, on its way from London to New York, by Libyan terrorists in December 1988, the British government redoubled its domestic counter-terrorist efforts against a broader range of threats. Parliament also responded to the rise of fundamentalist religious terrorist groups by passing the Anti-Terrorism, Crime, and Security Act in 2001, an action that was criticized by many civil-rights groups.

Authorities in Northern Ireland detained suspected terrorists from the late 1950s onward during the IRA's "border campaign" of bombings. With a new wave of bombings under the IRA beginning in the late 1960s, including 153 bombings in 1970 alone, British authorities detained 2,000 suspected IRA members between 1971 and 1975. After bombs exploded in two pubs in Birmingham, England in November 1974, killing 21 and injuring 162 others, Parliament passed the Prevention of Terrorism (Temporary Provisions) Act of 1974. The act allowed authorities to arrest suspected terrorists without a warrant and detain them for up to a week without filing charges against them. Suspected terrorists could also be deported from England to Northern Ireland.

The policy of internment raised international criticism, as did the practice of "hooding," in which detainees would be isolated and forced to wear hoods over their heads. After an investigation by the European Commission of Human Rights in 1976, the practices of food and sleep deprivation, noise bombardment, forced standing at attention, and hooding were condemned by the body. Despite the commission's decision, the practices continued. Some historians assert that the counter-terrorist policies contributed to an increase of IRA violence in retribution, as 2,161 people died in the 1970s in the conflict between the IRA and British authorities.

Whereas the counter-terrorist campaign against the IRA relied on military force, surveillance, and other covert and overt measures, there was a notable emphasis on technology in the wake of the Pan Am Flight 103 bombing in 1988. Libyan terrorists had successfully hidden plastic

explosives on the flight, which sent the aircraft plummeting into the village of Lockerbie, Scotland, after they detonated. In response, the British Airports Authority (BAA) undertook an extensive reevaluation of its security measures. The BAA reforms resulted in a five-stage system to screen all checked baggage at British airports, including x-ray machines and later, three-dimensional scanners and equipment that could detect trace elements of explosive devices. All passengers at BAA airports were also screened through x-ray machines and metal detectors and a predetermined number of passengers were individually hand searched by security officers. All carryon items were also x-rayed and articles that failed to pass inspection were individually inspected. Although the measures were sufficient to prevent terrorists from attacking a BAA facility or the planes that ran through them, a series of robberies in 2002 on BAA runways demonstrated that the system still had flaws.

In December 2001, British Parliament passed the Anti-Terrorism, Crime, and Security Act. The law allowed authorities to detain suspected terrorists for up to six months without filing charges and for additional six-month periods after reviewing the suspect's case. It also retained provisions that made it a crime to fail to report information on terrorist activities. In order to allay fears of civil-rights advocates, a provision was added to limit the powers of police and other security services from looking through confidential records.

### ■ FURTHER READING:

#### BOOKS:

English, Richard. *Armed Struggle: A History of the IRA*. New York: Oxford University Press, 2003.

Geraghty, Tony. *The Irish War: The Hidden Conflict between the IRA and British Intelligence*. Baltimore: Johns Hopkins University Press, 2000.

Gerson, Allan. *The Price of Terror: Lessons of Lockerbie for a World on the Brink*. New York: HarperCollins, 2001.

Taillon, J. Paul de B. *The Evolution of Special Forces in Counter-terrorism: The British and American Experiences*. Westport, Conn.: Greenwood Publishing Group, 2000.

#### ELECTRONIC:

British Airports Authority. "About BAA." <[http://www.baa.co.uk/main/corporate/about\\_baa/our\\_business/security\\_page.html](http://www.baa.co.uk/main/corporate/about_baa/our_business/security_page.html)> (March 5, 2003).

Human Rights Watch. "U.K.: New Anti-Terror Law Rolls Back Rights." <<http://www.hrw.org/press/2001/12/UKbill1214.htm>> (March 5, 2003).

#### SEE ALSO

*Airline Security*

*Bomb Detection Devices*

*Intelligence and Democracy: Issues and Conflicts*

*Interrogation: Torture Techniques and Technologies*

*MI5 (British Security Service)*

*MI6 (British Secret Intelligence Service)*

*Pan Am 103 (Trial of Libyan Intelligence Agents Interrogation: Torture Techniques and Technologies*

## United Kingdom, Intelligence and Security

The intelligence community of the United Kingdom is both older and more complicated than that of the United States. MI5, or the Security Service, and MI6, the Secret Intelligence Service, are the best-known components of the British intelligence structure, but these are just two parts of a vast intelligence apparatus. Command and control operates through no less than four entities: the Central Intelligence Machinery, the Ministerial Committee on the Intelligence Services, the Permanent Secretaries' Committee on the Intelligence Services, and the Joint Intelligence Committee. Communications intelligence is the responsibility of the Government Communications Headquarters (GCHQ), which works closely with the Communications Electronics Security Group, while a number of agencies manage military intelligence under the aegis of the Ministry of Defense. Even London's Metropolitan Police, or Scotland Yard, has its own Special Branch concerned with intelligence.

The principal oversight committee for British intelligence is the Central Intelligence Machinery, based in the Prime Minister's Cabinet Office. Roughly analogous, in various ways, to the U.S. National Security Council, Intelligence Community, and intelligence committees in both houses of Congress, it oversees the coordination of security and intelligence agencies. The Central Intelligence Machinery acts as a mechanism for assessment and accountability, observing and reporting on the performance of specific agencies. It is also concerned with tasking and the allocation of resources.

Whereas the Central Intelligence Machinery is at the top echelon of command and control, the Ministerial Committee on the Intelligence Services exercises regular ongoing oversight of intelligence activities. Through this committee, the Prime Minister, with the assistance of the Secretary of the Cabinet, exercises authority over the daily operations of the British intelligence and security communities as a whole. The Home Secretary oversees MI5, the National Criminal Intelligence Service, and Scotland Yard, while MI6 and GCHQ answer to the Foreign and Commonwealth Secretary.

These ministers receive assistance from the Permanent Secretaries' Committee on the Intelligence Services. Finally, the Joint Intelligence Committee, or JIC, is not unlike America's National Intelligence Council, which prepares National Intelligence Estimates. JIC draws up general intelligence needs to be met by GCHQ and MI6.

**MI5 and domestic security.** The "MI" by which the two principal British security services are known (MI5, or Security Service, and MI6, or Secret Intelligence Service) refers to their common origins in military intelligence. Both can trace their roots to the Secret Service Bureau, created in 1909 after a report by Parliament's Committee on Imperial Defense concluded that "an extensive system of German espionage exists in this country. . ." Working with the War Office, Admiralty, and various operatives and agents overseas, the bureau had both a Home Section and a Foreign Section—precursors, respectively, of MI5 and MI6.

After the outbreak of World War I, the War Office took over the Home Section, designated MI5 in 1916. MI5, which might be likened to the U.S. Federal Bureau of Investigation (although its operatives do not have arrest powers), spent the war years successfully apprehending a number of German spies and saboteurs in England, and after the war directed its attention against Communist elements. By the late 1930s, MI5's focus once again became German and pro-German infiltrators, of which it captured several. During the Cold War, MI5 returned to the efforts against Communists that had concerned it in the interwar years, but was less successful in this, due to the discovery of numerous Soviet moles within its ranks. Today, MI5 is concerned with counter-terrorism and counter-espionage against groups in Northern Ireland, as well as terrorist organizations based in the Middle East and other parts of the world.

**Scotland Yard.** The Metropolitan Police is better known by a name that refers to the location of its original headquarters, which overlooked a residence formerly owned by Scottish royalty. Scotland Yard, established in 1829, has a number of intelligence and surveillance units. Among these is the Scientific Intelligence Unit, which is concerned with behavioral and DNA analysis relating to unsolved crimes. The unit scored a major victory in 1986, when it became the first police organization in the world to track down a rapist and murderer—the perhaps appropriately named Colin Pitchfork—by use of DNA evidence.

Scotland Yard formed the world's first antiterrorism unit in 1883, when it established the Special Irish Branch in response to bombings in London committed by the Irish Fenian movement. The office later became known as the Special Branch. Providing protective services for Queen Victoria and later monarchs, the Special Branch performed a function akin to that of the U.S. Secret Service. The Special Branch also assists MI5 with a number of activities that include surveillance, arrest (a power that Special Branch officers possess), and testimony at trial. This last duty helps preserve the cover of MI5 officers, who are rarely allowed to testify in public to minimize risk of exposure.

**National Criminal Intelligence Service.** In addition to its other responsibilities, Scotland Yard operates the National Identification Service, which includes the National Criminal

Record Office and National Fingerprint Collection. Despite these efforts at gathering criminal intelligence, in the 1980s the Home Secretary's office recognized the need for better coordination of these intelligence-gathering efforts, and in April 1992, established the National Criminal Intelligence Service (NCIS).

Directed toward criminal organizations operating within the country, NCIS is one of Europe's first national criminal intelligence services. Its staff of some 500 personnel has backgrounds in police, customs, and excise work. Its areas of interest range from organized crime, drug trafficking, and money laundering to child molestation and football hooliganism.

**MI6 and international intelligence.** MI6 (formerly the Secret Service Bureau Foreign Section) gained its present designation in 1921. From it would emerge the precursor to GCHQ in 1919. Analogous to the U.S. Central Intelligence Agency (CIA), MI6 directed its efforts toward more or less the same threats targeted by MI5: Germans during the world wars, and Communists during the interwar and postwar periods. In World War II, MI6 sponsored aerial reconnaissance efforts that would later be taken over by the Royal Air Force (RAF).

Through GCHQ, MI6 enjoyed a number of successes during World War II, most notable among them being the Ultra program to break German Enigma ciphers. Like MI5, however, MI6 in the early Cold War experienced embarrassment with the exposure of Soviet spy rings operating in its midst. Yet MI6 also scored a victory by cultivating a Soviet mole in Oleg Penkovsky, who went on to work with both MI6 and CIA. Whereas MI5 established an atmosphere of openness in the post-Cold War era, MI6, which continues to operate extensively abroad, remains highly secretive.

**GCHQ.** GCHQ grew out of the Government Code and Cypher School (GC&CS), established in November 1919. During the 1920s and 1930s, GC&CS had considerable success in its efforts to decipher German and Soviet transmissions. Once the Germans acquired the Enigma machine, with its apparently unbreakable ciphers, in the late 1930s, GC&CS greatly stepped up its efforts. In August 1939, just before war broke out in Europe, it moved its headquarters to Bletchley Park outside London. There its cryptanalysts undertook Operation Ultra, the breaking of the Enigma cipher—a project whose details remained classified until the 1970s.

Renamed the Government Communications Headquarters in 1942 to conceal its activities, this leading communications intelligence agency of the United Kingdom—quite similar in function to the U.S. National Security Agency (NSA)—greatly escalated its efforts in the Cold War. GCHQ is also like NSA, with which it participates in the Echelon global surveillance network, in its level of secrecy. Much of what is known about it comes from

James Bamford's famous 1982 book on NSA, *The Puzzle Palace*.

According to Bamford, GCHQ at that time had six directorates. Among these were the Composite Signals Organization, dedicated to radio intercepts; the Directorate of Organization and Establishment, whose functions were chiefly administrative; the Directorate of Signals Intelligence Plans, concerned with long-range planning and management; and the Joint Technical Language Service, which intercepted foreign communications. The Directorate of Signals Intelligence Operations and Requirements, which was the largest and most secretive of directorates, according to Bamford, oversaw codebreaking activities.

Bamford also named the Directorate of Communications Security, whose activities were affiliated with an agency about which somewhat more is known, the Communications Electronics Security Group, or CESG. Established in 1969, CESG is the British national technical authority for information security, and works with a number of government agencies to ensure that communications security is maintained through state-of-the-art equipment. At the end of the Cold War, GCHQ employed some 6,000 people, but its staff had decreased to about 4,500 by the mid-1990s.

**Military intelligence.** In addition to the Cabinet-level oversight committees mentioned earlier, the Minister of Defense controls military intelligence through the Defence Procurement Executive and the Defense Intelligence Staff (DIS). DIS in turn oversees a number of military intelligence agencies, most notably the Defense Geographic and Imagery Intelligence Agency (DGIA) and the Defense Intelligence and Security Center.

DGIA was formed in 2000 from the merger of the RAF's Joint Air Reconnaissance Intelligence Center (JARIC) and the Military Survey Defense Agency. JARIC was concerned with aerial reconnaissance and the capture of photographic intelligence, and the Military Survey with geographic and geospatial support to defense planning. The Defense Intelligence and Security Center, created in 1996, integrates intelligence and security training for Britain's military services.

#### ■ FURTHER READING:

##### BOOKS:

- Aldrich, Richard J. *The Hidden Hand: Britain, America, and Cold War Secret Intelligence*. Woodstock, NY: Overlook Press, 2002.
- Andrew, Christopher M. *Her Majesty's Secret Service: The Making of the British Intelligence Community*. New York: Viking, 1986.
- Bamford, James. *The Puzzle Palace: A Report on America's Most Secret Agency*. Boston: Houghton Mifflin, 1982.

Bar-Joseph, Uri. *Intelligence Intervention in the Politics of Democratic States: The United States, Israel, and Britain*. University Park: Pennsylvania State University Press, 1995.

Dorril, Stephen. *MI6: Inside the Cover World of Her Majesty's Secret Intelligence Service*. New York: Free Press, 2000.

Pincher, Chapman. *The Spycatcher Affair*. New York: St. Martin's Press, 1988.

Polmar, Norman, and Thomas B. Allen. *Spy Book: The Encyclopedia of Espionage*. New York: Random House, 1998.

West, Nigel. *Molehunt: Searching for Soviet Spies in MI5*. New York: W. Morrow, 1989.

Winterbotham, F. W. *The Ultra Secret*. New York: Harper & Row, 1974.

Wright, Peter. *Spycatcher: The Candid Autobiography of a Senior Intelligence Officer*. New York: Viking, 1987.

#### ELECTRONIC:

Communications Electronics Security Group. <<http://www.cesg.gov.uk/>> (April 12, 2003).

Government Communications Headquarters. <<http://www.gchq.gov.uk/>> (April 12, 2003).

The Metropolitan Police Service. <<http://www.met.police.uk/>> (April 12, 2003).

MI5: The Security Service. <<http://www.mi5.gov.uk/>> (April 11, 2003).

United Kingdom Intelligence Agencies. Federation of American Scientists. <<http://www.fas.org/irp/world/uk/index.html>> (April 11, 2003).

#### SEE ALSO

*Bletchley Park*

*British Terrorism Act*

*Echelon*

*MI5 (British Security Service)*

*MI6 (British Secret Intelligence Service)*

*Official Secrets Act, United Kingdom*

*Special Relationship: Technology Sharing Between the Intelligence Agencies of the United States and United Kingdom*

*Ultra, Operation*

*United Kingdom, Counter-terrorism Policy*

*United States, Intelligence and Security*

among nations. The Security Council fulfills the UN mission through diplomacy, sanctions, and peacekeeping operations.

**Membership, organization, and voting.** The United Nations is divided into one large meeting body, the General Assembly, and three smaller operational committees. Every member nation, as well as observer missions, is represented in the General Assembly, and on two committees, the Economic and Social Council and the Trusteeship Council. Membership in the third and most powerful UN committee, the Security Council, is selected by established protocol. Five nations, reflecting the global balance of power when the United Nations was created, have permanent membership on the Security Council: the United States, Britain, France, Russia, and China. The ten other seats on the Security Council are filled by UN member states on a rotating basis, for two terms. The presidency of the Security Council changes every month, rotating according to the English alphabetical listing of represented countries.

The Security Council itself is divided into two standing committees, the Committee of Experts on Rules of Procedure and the Committee on the Admission of New Members. The council contains several *ad hoc* committees, which are created to draft resolutions, investigate issues, and mediate conflicts. Working groups are often formed to conduct preliminary, investigative research on a resolution, or to facilitate the evolution of policy regarding a long-standing crisis.

In the UN General Assembly, each member state has one vote. The same applies to voting on resolutions within the Security Council. Passage of a resolution requires either a simple majority or a two-thirds majority, depending on the rule of parliamentary procedure under which the vote was called. However, the permanent members of the Security Council reserve special voting rights. Permanent members reserve the right of veto, or the ability to strike down resolutions with their singular vote.

Under the rules of the UN charter, the Security Council must meet at least once every year. However, the Security Council is designed to operate continuously. The non-permanent seats have staggered terms, so that the council changes five members every year, instead of ten members every two years. One member of each national delegation to the Security Council must be present at the United Nations at all times so the council can meet on a moments notice. On the few occasions that the council has met at a location other than the United Nations, Security Council member states observed this rule by leaving a member of their delegation at headquarters.

**Duties of the Security Council.** The Security Council's main objective is the promotion of peace. To that end, the council has at its disposal several means of dispute resolution, ranging from mediation to military action. When a threat against international peace is brought to the attention of the Security Council, the council first attempts to

## United Nations Security Council

■ ADRIENNE WILMOTH LERNER

The United Nations Charter was ratified by its founding members on October 24, 1945. Three years later, the member nations convened the first official meeting of the Security Council, as well as the other UN committees. The outstanding mission of the entire United Nations organization is to promote global peace and good relations



The United Nations Security Council stands to observe a moment of silence during their meeting on September 12, 2001. The council approved a draft resolution condemning the terrorist attack on New York's World Trade Center. ©AFP/CORBIS.

negotiate a settlement between the disputing parties. The council may use its own member delegations, refer the issue to discussion in the General Assembly, or appoint the Secretary-General, the head of the United Nations, to act as mediator.

If no peaceful agreement can be reached, and the disputing factions use violence, intimidation, or force, the Security Council can then enact policy resolutions to solve the conflict or restore peace. Sometimes this policy includes economic sanctions, such as trade embargoes or prohibitions on governments borrowing from international funds. Under the Security Council regulations, however, humanitarian aid can never be withheld from any nation or group of people. In the past, the United Nations has applied sanctions to nations in violation of non-proliferation of weapons agreements, or whose governments perpetuated human rights crimes. The Security Council also reserves the right to recommend expulsion of any UN member state in gross violation of the UN charter and international law, though the dismissal must be voted on and passed in the General Assembly.

The Security Council is the only United Nations organization that can authorize military action and maintain a military-trained peacekeeping force. In violent international dispute, the Security Council can send intervening peacekeeping troops to secure areas in turmoil.

Peacekeeping forces are supplied by various individual UN member states but under the direction of UN command. Peacekeeping forces do not participate in the military agenda of any specific member state, and are neutral in all disputes. The role of peacekeeping troops in the international community is to preserve order, to protect civilian infrastructure and safety, and guard the delivery of humanitarian aid to better facilitate the diplomatic resolution of conflicts.

The Security Council is further responsible for overseeing compliance with international agreements involving weapons, the rules of engagement (conduct during war), the illegal spread of nuclear technology, and other threats to international peace. To enforce these treaties, such as international agreements on nuclear non-proliferation, the Security Council can authorize UN-led inspections of a nation's military arsenal. In addition, the Security Council can order sanctions or authorize military action.

**Impact on the international community.** Actions taken by the United Nations Security Council have had a significant impact on the international community, with varying success. Long-standing sanctions against South Africa helped end the nation's practice of apartheid and rehabilitated its standing in the international community. On the other

hand, resolutions and UN mandates regarding the Palestinian-Israeli conflict have been frequently breached, and those enforced failed to abate violence in the region. In the past decade, the Security Council has intervened in conflicts in from Bosnia to western Africa. Though peacekeepers in most tumultuous regions have managed to help dissemination of humanitarian aid and enforce the rule of law, root diplomatic solutions have lagged behind.

In 2002 and 2003, the UN Security Council was at loggerheads over the question of Iraq. Although the entire Assembly voted in favor of weapons inspections in the nation, the issue of subsequent military intervention was contentious. The United States and Great Britain, as well as other UN member nations, opted to invade Iraq to overthrow the regime of Saddam Hussein without the express consent of a new, specific Security Council resolution, but with the implied consent of previous Resolution 1441. However, United Nations organizations have continued to provide humanitarian aid to the region.

In early 2003, the Security Council supervised fifteen ongoing peacekeeping missions and considered resolutions seeking to implement more. In its almost sixty-year tenure, the Security Council has authorized 55 separate peacekeeping operations. Holding to the principles of the UN charter, many nations participate in ongoing peacekeeping efforts.

■ FURTHER READING:

ELECTRONIC:

United Nations. <<http://www.un.org>> (1 April 2003).

OTHER:

United Nations. *Sources: Basic Facts about the United Nations*. Sales No.E.98.I.20., Press Release GA/9784, 2000.

SEE ALSO

*Bosnia, Intelligence and Security*  
*IMF (International Monetary Fund)*  
*Nonproliferation and National Security, United States*  
*Weapons of Mass Destruction, Detection*  
*World War II*

---

## United Self-Defense Forces/ Group of Colombia (AUC *Autodefensas Unidas de Colombia*)

---

The United Self-Defense Forces/Group of Colombia (AUC *Autodefensas Unidas de Colombia*)—commonly referred to as the paramilitaries—is an umbrella organization formed in April 1997 to consolidate local and regional paramilitary

groups each with the mission to protect economic interests and combat insurgents locally. AUC is supported by economic elites, drug traffickers, and local communities lacking effective government security. AUC claims its primary objective is to protect its sponsors from insurgents. The AUC now asserts itself as a regional and national counterinsurgent force. It is adequately equipped and armed and reportedly pays its members a monthly salary. AUC political leader Carlos Castaño has claimed 70% of AUC's operational costs are financed with drug-related earnings, the rest from "donations" from its sponsors.

**Organization activities.** AUC operations vary from assassinating suspected insurgent supporters to engaging guerrilla combat units. Colombian National Combat operations generally consist of raids and ambushes directed against suspected insurgents. The AUC generally avoids engagements with government security forces and actions against U.S. personnel or interests.

The AUC is estimated to have 6000 to 8150 members, including former military and insurgent personnel. AUC forces are strongest in the northwest in Antioquia, Córdoba, Sucre, and Bolívar Departments. Since 1999, the group demonstrated a growing presence in other northern and southwestern departments. Clashes between the AUC and the Revolutionary Armed Forces of Colombia (FARC) insurgents in Putumayo in 2000 demonstrated the range of the AUC to contest insurgents throughout Colombia.

■ FURTHER READING:

ELECTRONIC:

Central Intelligence Agency. *World Factbook*, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. *Patterns of Global Terrorism 2001*, Annual Report: On the Record Briefing. May 21, 2002 <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).

U.S. Department of State. *Annual Reports*. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).

SEE ALSO

*Terrorism, Philosophical and Ideological Origins*  
*Terrorist and Para-State Organizations*  
*Terrorist Organization List, United States*  
*Terrorist Organizations, Freezing of Assets*

---

## United States, Counter- Terrorism Policy

---

■ JUDSON KNIGHT

The foundation of the United States counterterrorism policy, according to the U.S. State Department Coordinator for Counterterrorism, are embodied in four principles:



The National Center for the Study of Counter-Terrorism and Cyber-Crime on the campus of Norwich University in Northfield, Vermont, when fully operational, will focus on security concerns from miniaturizing communications devices to combatting attacks on computer networks. AP/WIDE WORLD PHOTOS.

the government makes no concessions to or agreements with terrorists; terrorists must be brought to justice for their crimes; states that sponsor terrorists and terrorism must be isolated and pressured so as to force a change of behavior; and the counterterrorism capabilities of countries allied with the United States, and those that require assistance in fighting terrorism, must be bolstered. President William J. Clinton outlined U.S. policy on terrorism in Presidential Decision Directive (PDD) 39 in 1995, and in 1998 he made specific provisions for combatting terrorism in PDD 62. Since the terrorist attacks of September 11, 2001, the face of U.S. counterterrorism has changed considerably, with the signing of the Patriot Act as well as a number of other measures. Among these is a refocusing of the nation's leading law enforcement organization, the Federal Bureau of Investigation (FBI), toward a mission increasingly concerned with counterterrorism.

## Deterrence and the Reduction of Vulnerabilities

These four principles provide a framework for U.S. policy. For example, when President George W. Bush sent U.S. troops into combat in Afghanistan in October 2001, and in Iraq in March 2003, this action was in line with the third principle, pressuring nations that support terrorism. Yet, even before September 2001, these principles were in

place, and have guided the policy of successive administrations, whether controlled by Republicans or Democrats.

Issued by Clinton on June 21, 1995, just two months after the Oklahoma City bombing, PDD 39 was titled "U.S. Policy on Counterterrorism." Its purpose was to provide guidelines for deterring terrorism on America's shores, as well as terrorism against Americans and allies abroad.

PDD 39 ordered the Attorney General, the Director of the FBI, the Director of Central Intelligence (DCI), and the secretaries of State, Defense, Transportation, and Treasury, to enact measures to reduce vulnerabilities to terrorism. Also critical in this regard are the General Accounting Office (GAO), whose responsibilities include national preparedness, and the General Services Administration (GSA), which, as overseer of government building projects, has been increasingly tasked toward providing structural protections against attacks such as those at Oklahoma City or the World Trade Center.

The directive, only part of which has been declassified, also addressed deterrence of terrorism. It called for the return of indicted terrorists to the United States for prosecution, and presented measures (classified as of 2003) for dealing with states that support terrorism. In PDD 62, issued on May 22, 1998, Clinton established the National Coordinator for Security, Infrastructure Protection and Counterterrorism, while PDD 63 created the Critical Infrastructure Assurance Office (CIAO).



Although the functions of CIAO and the national coordinator were similar, they reported along quite different chains of command. Whereas CIAO, now part of the Department of Homeland Security (DHS), was then part of the Department of Commerce, the national coordinator reported to the National Security Council (NSC). Given the fact that the NSC is the president's advisory board on national security affairs, this fact signaled the importance of the new national coordinator.

**The Patriot Act.** The leading statement of deterrence policy since September 2001, is the Patriot Act, which Bush signed into law on October 26, just six weeks after the attacks. The law contained changes to some 15 different statutes, and its provisions collectively gave the Justice Department and its agencies a number of new powers in intelligence-gathering and criminal procedure against drug trafficking, immigration violations, organized criminal activity, money laundering, and terrorism and terrorism-related acts themselves.

Among its specific provisions, the Patriot Act gave increased authority to intercept communications related to an expanded list of terrorism-related crimes; allowed investigators to aggressively pursue terrorists on the Internet; provided new subpoena power to obtain financial information; reduced bureaucracy by allowing investigators to use a single court order for tracing a communication nationwide; and encouraged sharing of information between local law enforcement and the Intelligence Community.

The Patriot Act also provided for the creation of a "terrorist exclusion list" (TEL). Members of organizations listed on the TEL may be prevented from entering the country, and in certain circumstances may be deported. Before the Secretary of State places an organization on the TEL, he or she must find that its members commit or incite terrorist activity, gather information on potential targets for terrorist activity, or provide material support to further terrorist activity.

## Assignments for Specific Agencies

In its provisions for responding to terrorism, PDD 39 designated the State Department as the lead agency for attacks on civilians outside of the United States. It also established the State Department Foreign Emergency Support Team (FEST) and the FBI's Domestic Emergency Support Team (DEST).

The directive gave the Federal Aviation Administration (FAA) authority to deal with "air piracy," and assigned authority over hijackings to the Department of Justice, working in concert with the departments of State, Defense, and Transportation. That particular part of PDD 39 has been superseded by the Aviation and Transportation Security Act (ATSA). Signed into law by President Bush on November 19, 2001, the ATSA created the Transportation

Security Administration (TSA), now part of the Department of Homeland Security (DHS).

In its consequence management provisions, PDD 39 gave the Federal Emergency Management Agency (FEMA) the responsibility of developing an overall federal response plan, and ensuring that states developed their own plans. This provision of PDD 39 is just one of many statements of policy on the coordination of consequence management responsibilities, which involve an array of departments, agencies, and offices, most notably FEMA, the Environmental Protection Agency (EPA), and the Coast Guard.

Nearly a decade earlier, for instance, Congress in 1986 passed the Emergency Planning and Community Right-to-Know Act (EPCRA), which established guidelines for assistance of local communities by federal agencies in the event of a toxic chemical spill or related incident. EPCRA also provides a framework for action both by citizens and state governments. Since the time of its passage, EPCRA and similar provisions have been increasingly understood to deal also with terrorist incidents, which may involve unleashing of lethal substances.

Similarly, in 1985, a FEMA committee had drawn up the Federal Radiological Emergency Response Plan (FRERP), a blueprint for the response of the U.S. federal government to a radiological emergency—that is, a crisis involving the release of nuclear radiation. The FRERP is an agreement among 17 federal agencies, key among which are FEMA, the Nuclear Regulatory Commission (NRC), the Departments of Energy and Defense, and the EPA.

Also important is the Coast Guard, which, in addition to protecting ports and shorelines, operates the National Response Center. The latter is the sole national point of contact for reports of oil spills, as well information regarding discharges of chemical, radiological, and biological discharges into the environment.

**Agencies tasked for counterterrorism.** Myriad government intelligence, security, and law enforcement agencies have a counterterrorism function. Most obvious among these are various components of the U.S. military, most notably Delta Force and Seal Team Six. These special teams, along with the larger Special Operations Command, are the "muscle" of U.S. counterterrorism. Highly trained and well-equipped with state-of-the-art weaponry, airborne insertion equipment, and other forms of technology, elite counterterrorist teams are capable of rescuing hostages and eliminating terrorists in situations for which regular military forces would be inappropriate.

Equally vital is the work of the Coordinator for Counterterrorism. In accordance with the fourth major principle of U.S. counterterrorism policy, the coordinator is charged by the Secretary of State with coordinating efforts to improve cooperation between the U.S. government and its foreign counterparts in battling terrorism. An ambassador, the coordinator is the primary functionary of the

federal government for developing and implementing America's counterterrorism policy.

**DCI Counterterrorist Center.** In an entirely different wing of government is the DCI Counterterrorist Center (CTC). Though part of the CIA, the CTC is under more direct control by the DCI than are most CIA activities, a sign of the significance attached to counterterrorism. During the mid-1980s, a panel led by then-Vice President George Bush studied U.S. efforts against terrorism and concluded that, while U.S. agencies collected information on foreign terrorism, they did not aggressively operate to disrupt terrorist activities. On these recommendations from Bush, himself a former DCI, William Casey established the CTC.

The mission of the CTC is to assist the DCI in coordinating the counterterrorism efforts of the Intelligence Community by implementing a comprehensive counterterrorist operations program, and by exploiting all sources of intelligence to produce in-depth analyses of terror groups and their state supporters. CTC collects information on these groups, and when it has credible information of a threat, issues warnings. Alongside it is the Interagency Intelligence Committee on Terrorism, an Intelligence Community board that assists the DCI in coordinating intelligence-gathering efforts against terrorists. In the 1990s, the CTC began working closely with the FBI, and in 1996 they exchanged senior-level officers to manage the counterterrorist offices of both agencies.

**The FBI.** Prior to September 2001, the mission of the FBI had been strictly that of a law-enforcement agency, but in the wake of September 11, Attorney General John Ashcroft and FBI Director Robert S. Mueller III refocused the bureau's efforts toward counterterrorism. In December 2001, Mueller announced plans to reorganize headquarters by creating new counterterrorism, cybercrimes, and counterintelligence divisions, by modernizing information systems, and emphasizing relationships with local first responders.

By the Spring of 2002, criticism of Mueller's plans was on the rise, with detractors maintaining that the measures were not thorough enough. To this end, Mueller announced a number of new reforms. These included the hiring of 400 more analysts, including 25 from the CIA; the retasking of 480 special agents from white-collar and violent crimes to counterterrorism; the creation of an intelligence office; development of terrorism expert support teams to work with the bureau's 56 field offices; recruitment of Arabic speakers and others fluent in Middle Eastern and South Asian languages; creation of a joint terrorism task force to coordinate with the CIA and other federal agencies; and the improvement of financial analysis and other forms of strategic analysis directed toward terrorist groups.

In January 2003, President Bush announced plans to create a new counterterrorism intelligence center that would bring together intelligence collected domestically

with that gathered overseas. This idea had been in development for some time, but one major issue of dispute was the question of which agency, the FBI or CIA, should manage the new center. One proposal put forward at the time involved the expansion of the DCI Counterterrorist Center, the oldest office of its kind. In February, Bush unveiled the organizational blueprint for the new unit, which would bring together FBI and CIA efforts under the aegis of a Terrorist Threat Integration Center, headed by the CIA.

## ■ FURTHER READING:

### BOOKS:

- Campbell, Kurt M., and Michele A. Flournoy. *To Prevail: An American Strategy for the Campaign against Terrorism*. Washington, D.C.: CSIS Press, 2001.
- Chapman, Robert, et. al. *COPS Innovations: A Closer Look: Local Law Enforcement Responds to Terrorism: Lessons in Prevention and Preparedness*. Washington, D.C.: U.S. Department of Justice Office of Community Oriented Policing Services, 2002.
- Combatting Terrorism: How Five Foreign Countries Are Organized to Combat Terrorism*. Washington, D.C.: General Accounting Office, 2000.

### PERIODICALS:

- Deutch, John. "Smarter Intelligence." *Foreign Policy* no. 128 (January/February 2002): 64–69.
- Eggen, Dan, and Jim McGee. "FBI Rushes to Remake Its Mission: Counterterrorism Focus Replaces Crime Solving." *Washington Post*. (November 12, 2001): A1.
- Eggen, Dan. "Bush Aims to Blend Counterterrorism Efforts." *Washington Post*. (February 15, 2003): A16.
- Haque, M. Shamsul. "Government Responses to Terrorism: Critical Views of Their Impacts on People and Public Administration." *Public Administration Review* 62 (September 2002): 170–80.
- Pincus, Walter, and Mike Allen. "Terrorism Agency Planned: Center to Integrate Intelligence, Analysis." *Washington Post*. (January 29, 2003): A12.

### ELECTRONIC:

- Coordinator for Counterterrorism. United States Department of State. <<http://www.state.gov/s/ct/>> (February 22, 2003).
- Counterterrorism Policy. University of Pittsburgh School of Law. <<http://jurist.law.pitt.edu/terrorism/terrorism2.htm>> (May 1, 2003).
- Terrorism/Counter-Terrorism Web Links. United States Institute of Peace. <<http://www.usip.org/library/topics/terrorism.html>> (May 1, 2003).

### SEE ALSO

- Canada, Counter-terrorism Policy*  
*Chemical and Biological Defense Information Analysis Center (CBIAC)*  
*Chemical safety: Emergency Responses*  
*Coast Guard National Response Center*

*Coordinator for Counterterrorism, United States Office  
DEA (Drug Enforcement Administration)  
Delta Force  
Domestic Emergency Support Team, United States  
Domestic Intelligence  
Domestic Preparedness Office (NDPO), United States  
National  
Emergency Response Teams  
France, Counter-terrorism Policy  
FEST (United States Foreign Emergency Support Team)  
EPA (Environmental Protection Agency)  
FEMA (United States Federal Emergency Management  
Agency)  
GAO (General Accounting Office, United States)  
General Services Administration, United States  
Germany, Counter-terrorism Policy  
Infrastructure Protection Center (NIPC), United States  
National  
Israel, Counter-terrorism Policy  
Law Enforcement, Responses to Terrorism  
National Preparedness Strategy, United States  
National Response Team, United States  
NNSA (United States National Nuclear Security  
Administration)  
Nuclear Emergency Support Team, United States  
Nuclear Regulatory Commission (NRC), United States  
SEAL Teams  
Security, Infrastructure Protection, and Counterterrorism,  
United States National Coordinator  
United Kingdom, Counter-terrorism Policy*

## United States, Intelligence and Security

■ JUDSON KNIGHT

The United States intelligence and security apparatus is a vast collection of departments, agencies, and offices. It is not a single monolithic entity, although within it is a unified, decentralized group of 14 intelligence and security organizations known as the Intelligence Community (IC). The Intelligence Community is overseen by the director of the Central Intelligence Agency (CIA), the most well known of intelligence organizations in the United States, and includes the nation's most prominent law-enforcement organization, the Federal Bureau of Investigation (FBI), as well as many others. In addition to the Department of Defense (DOD), entities involved in national security include the departments of Justice, the Treasury, Homeland Security (DHS), Energy, Commerce, and Transportation. In terms of national security as a whole, departments such as Agriculture, Health and Human Services, and the Interior also have a role to play, as do independent agencies, including the Federal Emergency Management Agency (FEMA), the Environmental Protection Agency (EPA), General Services Administration (GSA), and General Accounting Office (GAO).

Oversight of the IC in particular, and intelligence and security activities in general, comes from both the executive and legislative branches of government. The President, acting partly through the National Security Council (NSC), oversees intelligence and acts as commander-in-chief of the armed forces, a key component of security. Additionally, both houses of Congress exert influence through intelligence committees, and through their ultimate control over intelligence and security budgets.

The power of Congress over intelligence and security is exerted at a greater remove than that of the president, whose Executive Office oversees the NSC and other functions. The NSC consists of the president, the vice president, and the secretaries of State and Defense. Leadership comes from the president, often acting with, or through, the Assistant to the President for National Security Affairs—a role better known by the informal title National Security Advisor. The NSC can and usually does involve other Cabinet-level departments with a stake in national security.

In addition to the NSC, offices at the White House associated with intelligence and security include the Senior Director for Intelligence Programs; the National Coordinator for Security, Infrastructure Protection, and Counterterrorism; and the Office of National Drug Control Policy.

Particularly critical is the President's Foreign Intelligence Advisory Board (PFIAB), which reviews the activities and performance of all agencies involved in intelligence and advises the president on its assessments. Under the aegis of the PFIAB is the three-member Intelligence Oversight Board, responsible for reviewing the legality and propriety of intelligence activities.

Among agencies that operate at a national level are the Chemical and Biological Defense Information Analysis Center, Interagency Operational Security Support Staff, National Interagency Counterdrug Institute/National Interagency Civil-Military Institute, the Security Policy Board, and the Technical Support Working Group.

## The Intelligence Community

Central to U.S. intelligence and security are the 14 members of the Intelligence Community (IC). In addition to the CIA, the IC includes 13 other agencies and organizations, of which most are part of DOD. DOD members of the IC include the Defense Intelligence Agency (DIA), National Security Agency (NSA), National Reconnaissance Office (NRO), National Imagery and Mapping Agency (NIMA), and the intelligence agencies of the Army, Navy, Air Force, and Marine Corps. Non-DOD members include the FBI (a part of the Justice Department), the United States Coast Guard (part of DHS as of 2003), the State Department's Bureau of Intelligence and Research, and the intelligence agencies of the Energy and Treasury departments.

These 14 organizations work separately and together in fulfillment of a number of functions. Their "customer base" includes the president, the NSC, and other officials of the executive branch. In meeting the needs of these



The Central Intelligence Agency "Fusion Center," a command and control office where action against terrorists is coordinated. ©ROGER RESSMEYER/CORBIS.

"customers," the IC produces and disseminates a variety of intelligence gathered through the four traditional methods of intelligence collection: human, signals, imagery, and measurement and signatures intelligence (HUMINT, SIGINT, IMINT, and MASINT respectively).

Intelligence collection is directed toward information on international terrorist and narcotics trafficking activities, as well as other hostile activities against the United States by foreign powers, organizations, persons, and/or their agents. Other areas of interest for the IC, and for the intelligence and security apparatus as a whole, include information on cyber warfare, threats to critical infrastructure, weapons of mass destruction, and international organized crime. Members of the IC are also, of course, involved in the conduct of "special activities," to use the IC term, which can and do involve covert action against entities deemed a threat to national security.

**CIA and DCI.** The modern security and intelligence apparatus had its beginnings after World War II, specifically with the National Security Act of 1947, which created CIA, DOD, and the NSC. Today the head of the CIA, the Director of Central Intelligence (DCI), also serves as principal intelligence advisor to the president, as well as director of the IC. He is also responsible for presenting the president with

the annual IC budget, which must win congressional approval.

Staff organizations outside the CIA, but under DCI control, include the National Intelligence Council, responsible for preparing national intelligence estimates, and the Community Management Staff, which assists DCI in his IC executive functions. DCI also chairs two advisory boards, the National Foreign Intelligence Board and the Intelligence Community Executive Committee.

The CIA is an independent government organization tasked with supporting the president, the NSC, and other members of the national security leadership by providing accurate, comprehensive, and timely foreign intelligence on national security topics. CIA also supports the Chief Executive and other officials by conducting counterintelligence operations, "special activities," and other duties relating to foreign intelligence and national security as directed by the president.

The CIA includes four directorates: Operations, responsible for collecting foreign intelligence, including HUMINT, and for overseeing the overt collection of intelligence domestically through persons or organizations who volunteer that information; Intelligence, which produces the bulk of CIA's finished intelligence, processed from raw data collected in the field; Administration, which provides

support to CIA activities through a number of administrative and technical offices; and Science and Technology, which also provides support, through research, development, acquisition, and operations of technical capabilities and systems.

## Defense Department

The vast Department of Defense, with its 3.2 million people (including active military, reservists, National Guard, and civilian personnel) includes several groups within the Intelligence Community, but a much greater portion of DOD lies outside the IC, with activities that fall under the heading of "security" rather than intelligence.

Among the key DOD components of the IC is the ultra-secret NSA, the nation's leading cryptologic organization, whose activities include eavesdropping and surveillance. Within it is the even more secretive Special Collection Service. NIMA and NRO are likewise secretive and concerned with surveillance, primarily through satellites. In fact, NRO's existence was not even known until 1992.

Additionally, DOD houses DIA and the intelligence services of the armed forces. Intelligence functions within the military services include the Army Intelligence and Security Command (INSCOM); the various organizations under the Air Combat Command; and the National Maritime Intelligence Center, which houses the intelligence activities of the Navy, Marine Corps, and Coast Guard. (The last of these, in wartime, is attached to DOD rather than DHS.)

**Unified commands and defense agencies.** In addition to the services, DOD is divided into nine unified commands. Among the latter are five with geographic areas of responsibility, and four with non-geographic areas of focus. These are the Joint Forces Command, concerned with training and new solutions to future challenges; Strategic Command, which controls missile, deterrence, space, and satellite systems; Special Operations Command, which comprises a number of special support teams, including the Navy SEALs, Army Special Forces, and Delta Force; and the Transportation Command, responsible for moving personnel and materials around the world.

DOD also includes 15 defense agencies, many of which are critical to national security. These include not only DIA, NIMA, and NSA, but also the Defense Security Service, Defense Security Cooperation Agency, Missile Defense Agency, Defense Advanced Research Projects Agency, Defense Information Systems Agency, and Missile Defense Agency.

## Justice, Treasury, and other Departments

A number of components of CIA are concerned with counterintelligence, or the use of intelligence resources to

identify, circumvent, and neutralize the intelligence activities of a foreign power. Likewise, the FBI has a major counterintelligence unit, the National Security Division. The FBI as a whole is concerned not just with federal law enforcement in the United States, but with intelligence-gathering in the Western Hemisphere.

In addition to the FBI, the Justice Department contains a number of other components involved with intelligence and security, among them the Drug Enforcement Administration (DEA), the National Drug Intelligence Center (NDIC), and the U.S. National Central Bureau, which coordinates with Interpol. As of 2003, Justice was also home to the Bureau of Alcohol, Tobacco, Firearms, and Explosives, formerly a part of Treasury.

The latter department remains home to a number of agencies concerned with the security of financial assets, and with intelligence regarding financial activities. Treasury intelligence functions are a part of the IC. The Commerce Department, though it has no IC members, contains a number of organizations concerned with intelligence or security, most notable among them being the Critical Infrastructure Assurance Office.

## State, Energy, Transportation, and Homeland Security

Among the State Department offices involved in the IC are the Bureau of Intelligence and Research, the Bureau for International Narcotics and Law Enforcement Affairs, the Office of the Coordinator for Counterterrorism, the Foreign Emergency Support Team, and the Bureau of Diplomatic Security. The Energy Department is inherently concerned with national security, inasmuch as it protects U.S. energy resources, and within it are intelligence components that belong to the IC. Most of these are part of the National Nuclear Security Administration, which is charged with protecting U.S. nuclear materials.

The Transportation Department houses the Federal Aviation Administration, which has had a particularly important function in national security since the terrorist attacks of September 11, 2001. Transportation was also briefly home to the Transportation Security Administration, which oversees airport security screeners and air marshals, but those functions were moved to DHS. The latter includes a number of other agencies that formerly belonged to other departments, among them the U.S. Secret Service, Customs Service, Immigration and Naturalization Service, Border Patrol, and the Federal Law Enforcement Training Center.

**Independent agencies.** Among independent agencies, GSA plays a role in the security of federal buildings, many thousands of which it manages. This role has been particularly critical since the terrorist bombings in Oklahoma

City in April 1995. GAO studies the efficiency of U.S. activities and accounts for expenditures. It issues some 1,000 reports a year, and since September 2001, its evaluations of security measures undertaken by the federal government have provided a key means for assessing the degree to which various agencies and departments are prepared—or not prepared—for terrorist threats.

FEMA and the EPA work with a number of agencies, including the Coast Guard, to respond to emergencies involving environmental hazards and similar threats. The United States has a number of entities concerned with emergency response, many of which work with state and local authorities. EPA and the Coast Guard co-chair the U.S. National Response Team, an interagency group charged with emergency response planning and coordination. In times of emergency involving threats to health, the Public Health Service is additionally a key component of the national response.

## ■ FURTHER READING:

### BOOKS:

- Jeffreys-Jones, Rhodri. *Cloak and Dollar: A History of American Secret Intelligence*. New Haven, CT: Yale University Press, 2002.
- Johnson, Loch K. *Secret Agencies: U.S. Intelligence in a Hostile World*. New Haven, CT: Yale University Press, 1996.
- Richelson, Jeffrey T. *The U.S. Intelligence Community*, fourth edition. Boulder, CO: Westview Press, 1999.

### ELECTRONIC:

- U.S. Intelligence and Security Agencies. Federation of American Scientists. <<http://www.fas.org/irp/official.html>> (April 29, 2003).
- U.S. Intelligence Community. <<http://www.intelligence.gov/>> (April 14, 2003).

### SEE ALSO

*Air Force Intelligence, United States*  
*Air Force Office of Special Investigations, United States*  
*Air Marshals, United States*  
*Arms Control, United States Bureau*  
*ATF (United States Bureau of Alcohol, Tobacco, and Firearms)*  
*Aviation Security Screeners, United States*  
*Chemical and Biological Defense Information Analysis Center (CBIAC)*  
*CIA (United States Central Intelligence Agency)*  
*Civil Aviation Security, United States*  
*Coast Guard (USCG), United States*  
*Coast Guard National Response Center*  
*Commerce Department Intelligence and Security Responsibilities, United States*  
*Communications System, United States National Coordinator for Counterterrorism, United States Office Counter-Intelligence*  
*Critical Infrastructure Assurance Office (CIAO), United States*

*Customs Service, United States*  
*DCI (Director of the Central Intelligence Agency)*  
*DEA (Drug Enforcement Administration)*  
*DARPA (Defense Advanced Research Projects Agency)*  
*Defense Information Systems Agency, United States*  
*Defense Security Service, United States*  
*Department of State Bureau of Intelligence and Research, United States*  
*Department of State, United States*  
*DIA (Defense Intelligence Agency)*  
*Diplomatic Security (DS), United States Bureau*  
*DOD (United States Department of Defense)*  
*DOE (United States Department of Energy)*  
*Domestic Emergency Support Team, United States*  
*Drug Control Policy, United States Office of National*  
*FEST (United States Foreign Emergency Support Team)*  
*FAA (United States Federal Aviation Administration)*  
*FBI (United States Federal Bureau of Investigation)*  
*Federal Protective Service, United States*  
*Foreign Assets Control (OFAC), United States Office*  
*General Services Administration, United States*  
*Homeland Security, United States Department*  
*Information Security (OIS), United States Office*  
*Infrastructure Protection Center (NIPC), United States National*  
*INSCOM (United States Army Intelligence and Security Command)*  
*Inspector General (OIG), Office of the Intelligence Community*  
*Intelligence Policy and Review (OIPR), United States Office*  
*Intelligence Support, United States Office*  
*Intelligence, United States Congressional Oversight*  
*International Narcotics and Law Enforcement Affairs (INL), United States Bureau*  
*Interpol (International Criminal Police Organization)*  
*Justice Department, United States*  
*Law Enforcement Training Center (FLETC), United States Federal*  
*Military Police, United States*  
*National Archives and Records Administration (NARA), United States*  
*National Response Team, United States*  
*NIC (National Intelligence Council)*  
*NSC (National Security Council)*  
*Navy Criminal Investigative Service (NCIS)*  
*NCIX (National Counterintelligence Executive), United States Office of the*  
*NDIC (Department of Justice National Drug Intelligence Center)*  
*NFIB (United States National Foreign Intelligence Board)*  
*NIMA (National Imagery and Mapping Agency)*  
*NIST (United States National Institute of Standards and Technology)*  
*NIST Computer Security Division, United States*  
*NMIC (National Maritime Intelligence Center)*  
*National Military Joint Intelligence Center*  
*NNSA (United States National Nuclear Security Administration)*  
*NRO (National Reconnaissance Office)*  
*NSA (United States National Security Agency)*  
*Nuclear Emergency Support Team, United States*  
*PFIAB (President's Foreign Intelligence Advisory Board)*  
*President of the United States (Executive Command and Control of Intelligence Agencies)*  
*Public Health Service (PHS), United States*  
*Secret Service, United States*  
*Security Policy Board, United States*

*Security, Infrastructure Protection, and Counterterrorism,  
United States National Coordinator  
Soldier and Biological Chemical Command (SBCCOM),  
United States Army  
Special Collection Service, United States  
Special Operations Command, United States  
Surgeon General and Nuclear, Biological, and Chemical  
Defense, United States Office  
Terrorist Organization List, United States  
Transportation Department, United States  
Treasury Department, United States  
USAMRICD (United States Army Medical Research Insti-  
tute of Chemical Defense)  
USAMRIID (United States Army Medical Research Insti-  
tute of Infectious Diseases)  
USSTRATCOM (United States Strategic Command)*

## United States Intelligence, History

■ MICHAEL J. O'NEAL

From its inception, the United States made use of spies. The nation's first spymaster, General George Washington, recognized the need for accurate intelligence during the Revolutionary War. In a letter written July 26, 1777, Washington wrote: "The necessity of procuring good intelligence is apparent & need not be further urged—All that remains for me to add is, that you keep the whole matter as secret as possible." From his experience as a British officer in the French and Indian war, he often relied on intelligence provided by Native Americans to keep his troops mobile and out of reach of the enemy.

Intelligence operations in the American colonies, though, predate the war. In 1765, after the British passed the hated Stamp Act, a confederation of dissident groups called the Sons of Liberty formed to harass the British. By 1772 the Sons of Liberty had evolved into the Committees of Correspondence, whose purpose was to share information in resisting colonial rule. In Boston, members of the committee, including Samuel Adams and John Hancock, patrolled the streets at night, observing the movement of British troops and warning rebels in the countryside of impending British raids that might turn up caches of arms and gunpowder. The Boston group learned that on one of these raids the British intended to arrest Adams and Hancock, but it was unclear whether troops leaving Boston would travel across land or up the seacoast. In an early instance of intelligence tradecraft, Paul Revere arranged a signal that would give the rebels in the countryside advance warning of the direction of the raid—lanterns hung in the steeple of Boston's Old North Church. His stratagem, "one if by land, two if by sea," was immortalized by Henry Wadsworth Longfellow in his poem *Paul Revere's*

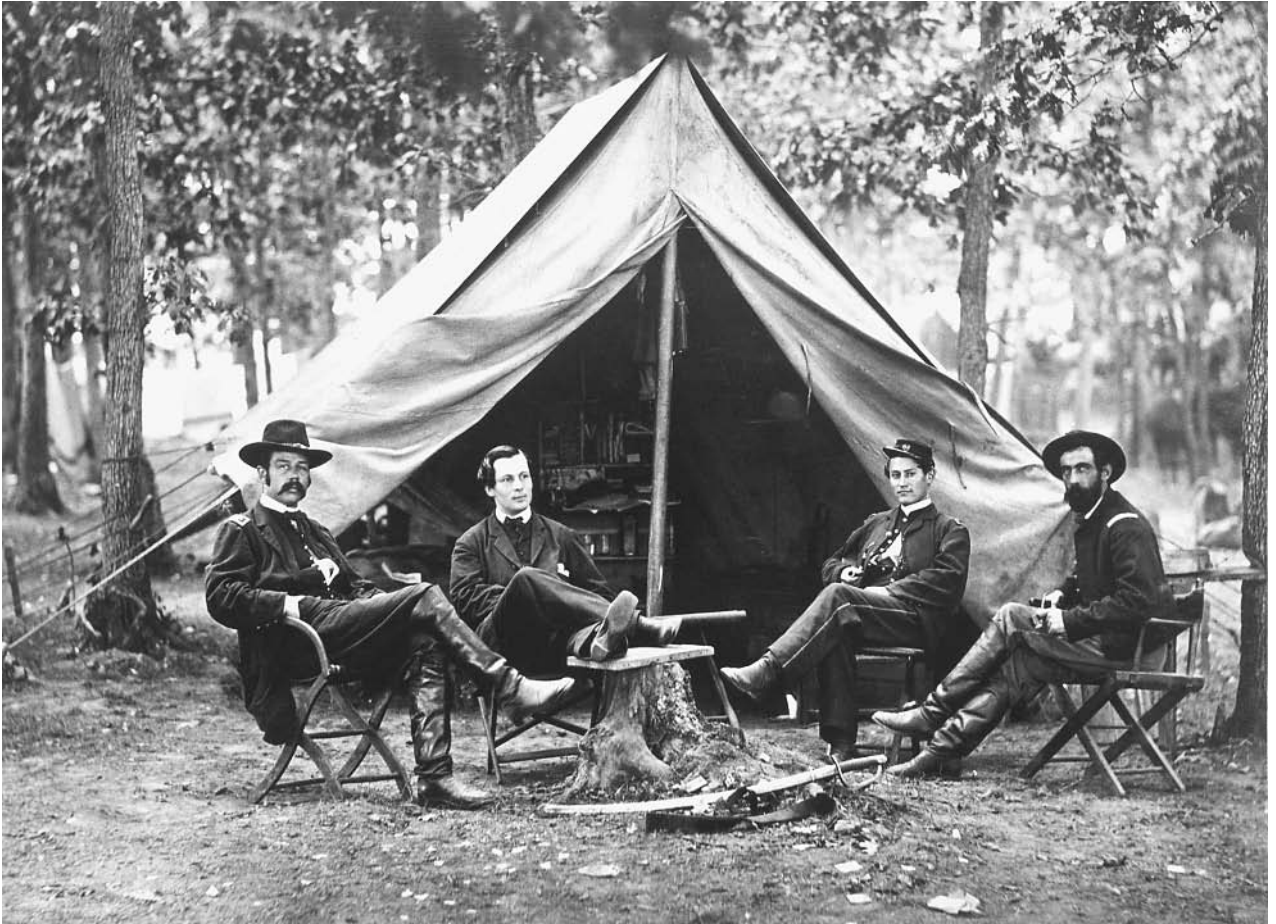
*Ride*. This raid went down in the history books as the Battles of Lexington and Concord, the opening salvos in the Revolution.

The Revolution also produced the new nation's first intelligence "mole" and the nation's first cryptanalyst. The mole was Dr. Benjamin Church, who posed as a member of the Boston group while secretly providing intelligence about American rebel activities to General Thomas Gage, commander of the occupying British troops in Boston. Later, as chief surgeon of the Continental Army, Church continued to funnel information to the British. He was finally exposed through a compromising letter he wrote in code. The letter eventually fell into the hands of Washington, who hired an amateur cryptanalyst, the Reverend Samuel West, to decipher it. Church was sent into exile and never heard from again.

Even Benjamin Franklin took part in spy games as head of the nation's first formal intelligence-gathering organization, the Committee of Secret Correspondence. Formed in 1775, the committee's principal goal was to gather information about sentiments toward the Revolutionary War in Europe. Franklin secretly negotiated with European powers to purchase arms and supplies. He also negotiated with France to procure the aid of French troops, whose arrival broke the war's stalemate and ultimately turned the tide in favor of the colonists.

In the decades following the Revolution, Americans adopted an isolationist stance and were absorbed with the task of building a nation, so they saw little need to take part in international espionage or to defend against it. As a result, the nation had few secrets, and the French, British, and Spanish in particular had little trouble learning American intentions. As tensions mounted again between Great Britain and the United States before the War of 1812, the British had secret agents throughout the country and even in the government itself. For its part, U.S. intelligence was so feeble that troops did not even have accurate maps of U.S.-Canadian border areas, the staging ground for British attacks. Even when U.S. authorities did acquire intelligence information, no one knew what to do with it. They knew, for example, that the British intended to burn Washington, D.C. No steps were taken to protect the capital.

**The Civil War.** Intelligence operations during the Civil War are wrapped today in an aura of romantic myth, perhaps because they represent the apex of the amateur spy. Legends in particular surround the efforts of women spies who often, according to legend, galloped across borders on horseback in the moonlight carrying to their brave men information concealed in their bodices. At the war's start, President Abraham Lincoln knew virtually nothing about the South's war-making capabilities. To gather intelligence, he, like Washington, became his own spymaster, running such men as William Alvin Lloyd, a transportation expert and publisher who moved freely about the South and provided valuable information about Southern troop



These officers with the Secret Service Department managed scouts and spies attached to the Army of the Potomac during the Civil War. ©CORBIS.

movements and the fortifications around cities like Richmond, Virginia. As an amateur, though, Lloyd developed no way to pass information in secret, and he even carried much of the information he gathered about with him on his person.

In the North, two rival intelligence organizations formed. One was run by the famous detective Allan Pinkerton, who reported to General George McClellan, commander of the Army of the Potomac. The other was headed by Lafayette Baker, who reported to General Winfield Scott and later to the secretary of state. These rival organizations often worked at cross-purposes, on occasion even arresting one another's members. While they frequently unearthed valuable information about Southern troop movements, officers assigned to intelligence work lacked experience and there was little coordination of their efforts. Too frequently, Northern commanders failed to act on the information they received.

The South, meanwhile, carried on widespread intelligence operations against the North, although again it is difficult to separate fact from fiction because when Richmond, the Confederate capital, fell, virtually all records of their operations were destroyed. Thus it remains an open

question, for example, whether John Wilkes Booth, Lincoln's assassin, was on the Confederate payroll as a spy. As an actor, he traveled freely throughout the cities of the North, giving him ample opportunity to meet with members of the network of spies the South had placed in New York City, Baltimore, Washington, Philadelphia, and other cities. In 1864 he played several engagements in Niagara Falls, New York, a hotbed of Southern espionage just over the border from Montreal. Montreal was the headquarters of the "Canadian Cabinet," a group of Southern leaders who directed espionage operations against the North. After fires broke out in several New York City hotels on November 25, 1864, a captured Southern agent confessed that the fires were the work of the Canadian Cabinet. Booth, it turned out, had been in Canada in the days preceding the arson raid and had met with the cabinet. Further, one of Booth's co-conspirators in the Lincoln assassination was John Surratt, a known Confederate spy and gun runner whose mother, Mary Surratt, was later hanged for her role in Lincoln's death.

**The beginnings of professional intelligence.** In the decades between the Civil War and World War I, the United States



took its first faltering steps toward development of an organized, professional intelligence capability. In 1885, President Grover Cleveland called for assignment of military attachés to foreign countries to gather information. During the Spanish-American War of 1898, the United States acquired—and most importantly, acted upon—human intelligence about Spain’s war-making capabilities. John Wilkie, head of the U.S. Secret Service, broke up the “Montreal spy ring” Spain had put in place in Canada. Before and during American participation in World War I, counterintelligence agents of the FBI and Secret Service were successful at ferreting out German agents and saboteurs within the United States, but during the war, the nation relied on cooperative arrangements with the British for overseas intelligence. It was the British, for example, who broke German diplomatic codes and in 1917 intercepted and deciphered the infamous Zimmermann telegram revealing Germany’s intention to begin unrestricted submarine warfare against the United States.

Between the two world wars, American intelligence again fell into abeyance. Typically, only inexperienced officers with little or no training in intelligence were sent to staff foreign embassies, so little valuable intelligence about Soviet, German, and Japanese intentions was acquired on the ground. Most U.S. intelligence was directed internally against radicals, subversives, communists, and anarchists during the “Red Scare” of the 1920s and against Nazi agents in the 1930s. The United States did, however, make strides in code breaking and began to develop an organized intelligence capability. In 1922, William Friedman, a Russian immigrant, was appointed chief cryptanalyst of the Army Signal Intelligence Service (SIS), which broke the Japanese Purple code, the principal cipher Japan used to send diplomatic messages as tension between the United States and Japan mounted. After the Japanese attack on Pearl Harbor on December 7, 1941, U.S. intelligence efforts focused on cracking Japan’s code for transmitting military messages. Leading the effort, code-named “Magic,” was the U.S. Navy’s Combat Intelligence Unit. Using complex mathematical analysis, IBM punch-card tabulating machines (the first example of cooperation between the military and private enterprise to gather intelligence), and a cipher machine, the unit was able to crack the code. Throughout World War II, the United States intercepted and decoded thousands of Japanese communications; cryptanalysts gave U.S. war planners advance notice of Japanese plans to attack Midway Island in June 1942, allowing U.S. forces to lie in wait, defeat the Japanese, and turn the tide in the Pacific.

**Modern U.S. intelligence.** The chief deficiency of U.S. intelligence during World War II was that it was scattered among the various branches of the military; whatever coordination it received happened only on President Franklin Roosevelt’s desk. To correct this deficiency, Roosevelt appointed William J. Donovan, a New York lawyer and former Army colonel, to assemble a plan for an intelligence service. Out of Donovan’s plan emerged the Office

of Strategic Services (OSS) in June 1942. Under Donovan’s leadership, the OSS was given the task of collecting and analyzing information needed by the Joint Chiefs of Staff and to conduct “special operations,” or clandestine operations that were not carried out by other federal agencies or the military. Throughout the war the OSS provided policy makers and the military with enemy troop strength estimates and other intelligence that was crucial to planning military campaigns.

The cold war with the Soviet Union following World War II gave increased urgency to the need for good intelligence, but opinion was divided about who should conduct intelligence operations and who should supervise their efforts. Roosevelt’s successor, Harry S. Truman, divided responsibilities between military and civilian agencies in October 1945 when he abolished the OSS and transferred its operations to the Departments of War and State. Donovan, though, favored the formation of a strictly civilian organization that would coordinate intelligence gathering. Fearing that the plan would lessen their influence, both the military and the FBI opposed it. Truman struck a middle course in January 1946 when he established the Central Intelligence Group (CIG), giving it the authority to coordinate intelligence gathered by existing departments and agencies. The CIG was placed under the supervision of a National Intelligence Authority, which consisted of the president and the secretaries of the State, War, and Navy departments. Thus, for the first time in its history the United States had a peacetime intelligence organization. Less than two years later, though, Congress passed the 1947 National Security Act, creating the civilian National Security Council (NSC) and placing under its authority the Central Intelligence Agency (CIA). Intelligence gathering was now firmly under the control of civilian rather than military authorities.

In the 1950s and early 1960s the CIA was the nation’s bulwark against the expansion of communism and Soviet influence. It was the CIA, for example, that revealed the presence of Soviet missiles in Cuba during the 1962 Cuban Missile Crisis. Its reputation was tarnished, though, by the disastrous Bay of Pigs operation against Cuban dictator Fidel Castro and reports of unsavory CIA activity during the war in Vietnam and, in the 1970s and 1980s, against unfriendly leftist regimes in Central and South America. After the terrorist attacks of September 11, 2001, the CIA took on added luster as the nation looked to it as the front line in the fight against terrorism.

In its early years the CIA relied primarily on human intelligence and field operations. Its science and technology efforts were scattered among various CIA divisions, or “directorates.” With the success of overhead intelligence-gathering technology, including the U2 spy plane and reconnaissance satellites, then CIA director John McCone wanted to gather all of the agency’s scientific and technological capabilities under one roof. The result was the formation of the Directorate of Science and Technology (DS&T) in 1963. Throughout its history, the DS&T has

enjoyed numerous successes, developing high-tech imagery and eavesdropping satellites and a host of other sophisticated tools that have proven invaluable in acquiring information while keeping American operatives out of harm's way.

## ■ FURTHER READING:

### BOOKS:

- Andrew, Christopher. *For the President's Eyes Only: Secret Intelligence and the Presidency from Washington to Bush*. New York: Harper Perennial, 1995.
- Kahn, David. *The Code-Breakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. New York: Scribner, 1997.
- Miller, Nathan. *Spying for America: The Hidden History of U.S. Intelligence*. New York: Paragon House, 1989.
- O'Toole, G. J. A. *Honorable Treachery: A History of U.S. Intelligence, Espionage, and Covert Action from the American Revolution to the CIA*. New York: Atlantic Monthly Press, 1991.
- Richelson, Jeffrey T. *A Century of Spies: Intelligence in the Twentieth Century*. New York: Oxford University Press, 1995.

### SEE ALSO

*CIA, Formation and History*  
*CIA Directorate of Science and Technology (DS&T)*  
*Civil War, Espionage and Intelligence*  
*Cryptology, History*  
*Cuban Missile Crisis*  
*Espionage and Intelligence, Early Historical Foundations*  
*National Security Act (1947)*  
*NSC (National Security Council), History*  
*Pearl Harbor, Japanese Attack on*  
*Revolutionary War, Espionage and Intelligence*  
*Spanish-American War*  
*War of 1812*  
*World War II, United States Breaking of Japanese Naval Codes*

## United States Oil Reserve.

SEE *Strategic Petroleum Reserve, United States*.

# Unmanned Aerial Vehicles (UAVs)

## ■ K. LEE LERNER

Israel was the first nation to make significant use of unmanned reconnaissance drones in combat during operations in Lebanon in 1982. The United States forces began

full deployment and use of unmanned aerial vehicles (UAVs) and related technology in the 1990s and UAVs—especially the Predator and Global Hawk—were extensively used by U.S. forces during Operation Enduring Freedom in Afghanistan and Operation Iraqi Freedom.

## Tactical Uses of UAVs

UAVs can fly in areas where air supremacy is not complete or air defenses have not been fully suppressed. UAV craft can also operate in biologically or chemically contaminated areas. In addition, UAVs offer a chance to conduct battle damage assessments—critical for further mission planning—without further risk to pilots.

As of May 2003 more than 1500 UAV sorties had been flown in Afghanistan and UAV craft destroyed, or assisted in the destruction of, nearly a thousand targets. In addition to the capability of some UAVs to fire Hellfire missiles, UAV can paint targets with lasers that guide other weapons systems.

## UAV Capabilities

The Predator flies at medium altitudes and is capable of long reconnaissance and surveillance missions. In conjunction with weapons systems, Predator craft are also used for target acquisition.

The Global Hawk, is capable of operating at higher altitudes (in excess of 60,000 ft) on and features an integrated sensor system that enhance its intelligence, surveillance, and reconnaissance capabilities.

The U.S. Navy operates the Pioneer UAV. Designed to operate over open ocean, the Pioneer design incorporates a low radar cross section and reduced infrared signature. Pioneer craft were first used during operations in Grenada and strikes against Libya.

The Shadow UAV offers day and night surveillance capability and can carry a 330 lbs. Payload while operating at 10,000 ft. The U.S. Army uses Shadow UAVs to call in or lock on (calibrate) artillery attacks.

UAV use has also spurred advances in miniaturized synthetic aperture radar that reduces weight but still offers high stationary and moving target resolution (i.e. radar that can discriminate targets separated by less than 18 inches (.5 m).

UAVs as platforms for weapons of mass destruction or terrorism. Prior to its being eliminated by U.S. forces, U.S. officials claimed that Saddam Hussein's Iraqi regime had developed and tested a limited number of UAVs capable of delivering biological agents.

In 2003, Hamas operatives were killed as they were preparing to test an unmanned aerial vehicle (UAV) purchased from illegal arms dealers. The craft exploded before Hamas could carry out a planned attack against a



The U.S. military used several unmanned spy aircraft such as this GNAT Aerial Reconnaissance Vehicle to help the Philippine military hunt down Islamist extremist guerrillas on the Philippine island of Basilan in 2002. AP/WIDE WORLD PHOTOS.

target inside Israel. Hamas spokesmen subsequently claimed that they been fooled into purchasing a booby-trapped UAV by the Israeli Security Agency ISA (Shin Bet).

Western press organizations have also carried reports that Palestinian agents have attempted purchases of model aircraft from suppliers in Europe with the intent to develop a crude but UAV capability. One factor limiting these types of operations is that typical hobbyist UAVs require line-of-sight control of the aircraft and are therefore incapable of navigating with precision over rugged terrain or over great distances.

**UAV use in intelligence operations and current research.** In November, 2002, a CIA-operated Predator operating over Yemen fired a missile that killed bin Laden's top lieutenant in Yemen, Qaed Salim Sinan al-Harethi, and five other al-Qaeda suspects.

DARPA planned advancement of the Unmanned Combat Air Vehicle (UCAV) and Unmanned Combat Armed Rotorcraft (UCAR) is designed to enhance the ability to

remotely suppress enemy air defenses, conduct extended surveillance in hostile territory, and pursue armed reconnaissance and attack missions.

A milestone in unmanned aviation, in 2002, the U.S. flew an unmanned plane on a trans-Pacific flight from California to Australia.

DoD and Northrop Grumman engineers are currently refining the Eurohawk for advanced electronics and signals intelligence operations. France is developing the Système de Drone Tactique Interimaire (SAGEM) and United Kingdom is developing a craft termed "Watch-keeper" to replace the Phoenix.

#### ■ FURTHER READING:

##### ELECTRONIC:

Airborne Autonomous Systems. Unmanned Aircraft. <<http://www.unmannedaircraft.com/>> (May 12, 2003).

American Forces Press Service, Garamone, Jim. "From U.S. Civil War to Afghanistan: A Short History of

UAVs." April, 16, 2002. <[http://www.defenselink.mil/news/Apr2002/n04162002\\_200204163.html](http://www.defenselink.mil/news/Apr2002/n04162002_200204163.html)> (May 12, 2003).

#### SEE ALSO

*Aviation Intelligence, History*  
*Balloon Reconnaissance, History*  
*Iraq War: Prelude to War (The International Debate Over the Use and Effectiveness of Weapons Inspections.)*  
*Persian Gulf War*  
*Weapons of Mass Destruction, Detection*

## UNSCOM (United Nations Special Commission).

SEE *Iraq War: Prelude to War (The International Debate Over the Use and Effectiveness of Weapons Inspections.)*

---

# Uranium

---

■ LARRY GILMAN

Uranium is a radioactive, metallic element with 92 protons and a variable number of neutrons in the nucleus of each atom. There are 16 isotopes of uranium, the most common being uranium-238 ( $^{238}\text{U}$ ). The second-commonest isotope of uranium,  $^{235}\text{U}$ , is used for building nuclear weapons, generating electricity, and propelling some submarines, aircraft carriers, and other vessels. Heat released by uranium decay also keeps Earth's interior hot, providing the energy for continental drift and volcanic eruptions.

Uranium was discovered in 1789 by German chemist Martin Heinrich Klaproth (1743–1817), and its property of radioactivity was discovered by French physicist Henri Becquerel (1852–1908) in 1896.  $^{235}\text{U}$  was first isolated in kilogram quantities by the United States during World War II, and was used in war by the United States in the bomb that destroyed the city of Hiroshima, Japan in 1945. Since that time uranium has been mined in many countries and purified in large quantities for both bombs and fuel. Worldwide, several hundred nuclear reactors produce electricity from uranium, while tens of thousands of nuclear weapons (mostly held by the United States and the Russian Federation) rely on uranium either as their primary explosive (in fission bombs) or as a trigger explosive (in fusion bombs).

Uranium atoms are unstable; that is, their nuclei tend spontaneously to fission or break down into smaller nuclei, fast particles (including neutrons), and high-energy photons. The fission of an isolated uranium nucleus is a randomly timed event; however, collision with a neutron

may trigger a uranium nucleus to fission immediately. Crowding large numbers of uranium atoms together can enable the neutrons emitted by a few nuclei undergoing fission to cause other nuclei to fission, whose released neutrons in turn trigger still other nuclei, and so on. If this chain reaction proceeds at a constant rate, it may be used to generate electricity; if it proceeds at an exponentially increasing rate, a nuclear explosion results.

Only 0.71% of natural uranium is  $^{235}\text{U}$ , the major isotope directly useful for nuclear power and weapons. Many tons of ore must therefore be refined to produce a single kilogram of  $^{235}\text{U}$ . The amount of  $^{235}\text{U}$  needed to make a bomb, however, is not great: about 15 lb (7 kg). Quantities of uranium sufficient for many thousands of bombs are thus available around the world; some 21 countries export uranium, with Canada, Australia, and Niger being the three largest producers.

The most common isotope of uranium,  $^{238}\text{U}$ , comprises 99.28% of the uranium in the Earth's crust.  $^{238}\text{U}$  is comparatively stable, with a half-life of 4.5 billion years, and so is not directly useful for power and nuclear weapons. It is added to some antitank and anti-aircraft ammunition to increase their density and thus their penetrating power. Depleted-uranium munitions, as these weapons are termed, were used extensively by the United States during the Gulf War of 1991 and in the Kosovo conflict of 1999. Because of their slight radioactivity, there is ongoing debate about whether they may cause long-term health problems in areas where they have been used.

$^{238}\text{U}$  is also a major ingredient of most reactor fuel. In reactor cores, this  $^{238}\text{U}$  is bombarded by neutrons, which transmute some of it into the element plutonium. Plutonium can be used directly for power and weapons; the first and third nuclear weapons ever exploded were produced by the United States using plutonium transmuted from  $^{238}\text{U}$ , and a number of other countries, including India, Israel, Pakistan, and North Korea, have developed the capability to obtain plutonium for bombs by the same means.

Both  $^{235}\text{U}$  and plutonium must be in fairly concentrated form for use in bomb manufacture. Alloys that have been diluted by  $^{238}\text{U}$  or other substances result in bulkier explosive devices; at sufficiently great dilution, a nuclear explosion is not obtainable. (However, some experts say that a nuclear explosion might be obtainable from an alloy that is as little as 10%  $^{235}\text{U}$ .) It follows that any organization that wishes to build an atomic weapon must either obtain fairly concentrated  $^{235}\text{U}$  or plutonium by purchase or theft, or obtain them in dilute form and then concentrate them.

These obstacles have been surmounted by a number of governments, and may eventually be surmounted by terrorist organizations. Illegal traffic in weapons-grade  $^{235}\text{U}$  and plutonium has accelerated since the breakup of the Soviet Union in 1991, because its successor states have been too poor and disorganized to keep nuclear material secure. Some 600 tons, or enough for about 40,000 bombs, of raw weapons-grade fissionables are



Weapons-grade uranium, captured near the Syrian border at Sanliurfa, Turkey, in September 2002, is displayed at the Sanliurfa paramilitary police headquarters. AP/WIDE WORLD PHOTOS.

stored in poorly guarded stockpiles in the Russian Federation and other states; small quantities have already entered the black market. On over 16 occasions since 1993, police in Asia, Europe, or South America have intercepted illegally held bomb-grade uranium or plutonium, most of it from ex-Soviet sources. In 1994, police seized a metal briefcase when a civilian jetliner from Moscow landed in Munich, Germany; the briefcase contained 363.4 grams of weapons-grade plutonium. In April 2000, almost a kilogram of bomb-grade uranium was seized in the Republic of Georgia. In 2001, police in Bogota, Colombia seized some 600 grams of bomb-grade  $^{235}\text{U}$  from the house of an animal feed salesman, the enrichment level of which corresponded to that of Russian fuel for submarines and icebreakers. And on September 11, 2001, four men were arrested in the ex-Soviet republic of Georgia in possession of almost 2 kilograms of bomb-grade  $^{235}\text{U}$ —a large fraction of the amount required for a bomb. Since that day, the idea that stolen uranium might be used for terrorist acts has gained increased attention.

Through its Material Protection, Control, and Accounting Program, the United States has spent about \$550 million since 1993 to help safeguard uranium and plutonium stocks in Russia, supplying complete security systems or partial protection for about a third of the material considered most vulnerable by the U.S. Department of Energy.

#### ■ FURTHER READING:

##### PERIODICALS:

Ladika, Susan. "Tracing the Shadowy Origins of Nuclear Contraband." *Science* no. 5522 (2001): 1634.

Stone, Richard. "Nuclear Trafficking: 'A Real and Dangerous Threat'." *Science* no. 5522 (2001): 1632–36.

#### SEE ALSO

*Nuclear Power Plants, Security*  
*Nuclear Reactors*  
*Nuclear Weapons*

## Uranium Depletion Weapons

■ LARRY GILMAN

Depleted uranium (DU) munitions are armor-piercing or general-purpose ammunition rounds that are composed, in part, of depleted uranium. Depleted uranium is uranium that has had most of its  $^{234}\text{U}$  and  $^{235}\text{U}$  removed for use in nuclear power or nuclear weapons, leaving metal that is almost entirely  $^{238}\text{U}$ .  $^{238}\text{U}$  is the least radioactive isotope of uranium, with a half-life of 4.46 billion years (6.3 times that of  $^{235}\text{U}$ ). It is used in munitions because of its density and hardness. The high density of DU (1.68 times that of lead, 2.43 times that of steel) allows it to transfer more kinetic energy to a target for a given round size than any other practically available metal. This, combined with its hardness, enables it to penetrate armor much more effectively than armor-piercing rounds made of other metals (e.g., tungsten). A typical armor-piercing DU round consists of a long, pointed shaft of DU that is surrounded by a sabot (from the French for "shoe"; a casing that fits the bore of the gun). When the round is fired, the sabot falls away, transferring some of its kinetic energy to the DU shaft.

When the shaft strikes end-on, its long, narrow shape concentrates all of the round's kinetic energy on a small area; as the round penetrates the armor it also tends, thanks to the particular mechanical properties of metallic uranium, to sharpen rather than to blunt or mushroom, further increasing its penetrating power.

DU is used not only for ammunition, but for ballast, gyroscope rotors, balancing weights on aircraft, armor enhancement, and in other applications calling for high-density material. The armor of the United States M1A1 Abrams Main Battle Tank, for example, consists of a layer of DU sandwiched between two layers of steel.

A variety of DU munitions have are in use by at least 20 technologically advanced military organizations around the world. The U.S. military leads both in quantities deployed and quantities used in combat. DU munitions were used by several branches of the U.S. military both in the Gulf War of 1991, in Bosnia-Herzegovina in 1994–95, and in Kosovo in 1999. During the Gulf War, U.S. forces fired 320 tons (290,300 kg) of DU munitions; during in Bosnia-Herzegovina, 3 tons (2721 kg); and in Kosovo, 10.2 tons (9253 kg). Much of this material remains on the ground.

There is no controversy about the military effectiveness of DU munitions. In an incident during the Gulf War, a U.S. Abrams tank with DU-enhanced armor was struck three times by main-gun rounds from three attacking Iraqi T-72 tanks. The Abrams remained operative despite the hits and responded with three DU main-gun rounds, destroying all three Iraqi tanks. Nevertheless, international debate has centered on the question of whether DU munitions pose a health hazard to military forces exposed to them during use or to civilian populations inhabiting regions contaminated by DU. There are two possible sources of health damage from DU: chemical toxicity and radioactivity.

**Chemical toxicity.** When a DU round strikes armor, it is pulverized and raised to a high temperature. Several oxygen-uranium compounds (uranium oxides) form under these conditions and can be harmful if inhaled or otherwise ingested (e.g., by direct penetration of the skin). Ingestion of sufficiently large quantities of uranium oxides can be harmful, especially to the kidneys. However, the U.S. government states that the quantities of uranium oxide that can be plausibly ingested under combat conditions, or by residents of contaminated areas, cannot be great enough to cause measurable health effects.

**Radioactivity.** The radioactivity of  $^{238}\text{U}$  is very low compared to that of  $^{235}\text{U}$ ; further, although DU contains trace quantities of elements that are more radioactive, such as  $^{235}\text{U}$ , americium, neptunium, plutonium, and technitium, these impurities increase DU's radioactivity by only about 0.8% over that of pure  $^{238}\text{U}$ . Most scientists agree that the DU radiation hazard to troops and civilian populations in contaminated areas is too low to measure. Nevertheless,

anecdotal reports of increased leukemia rates and other health problems in veterans exposed to DU have caused enough concern to trigger investigations of DU health effects by the United Nations Environmental Programme and several governments.

Although no ill effects from DU exposure have yet been definitely established by any study, the U.S. Department of Veterans Affairs is now tracking the health of veterans exposed to DU. Furthermore, the International Committee of the Red Cross has urged all countries that use DU munitions to review whether they comply with international agreements that forbid "weapons, means, or methods of warfare of a nature to cause superfluous injury or unnecessary suffering, which have indiscriminate effects, or which cause widespread, long-term and severe damage to the natural environment." Several such studies are now being pursued by European governments and by the U.S. government.

#### ■ FURTHER READING:

##### ELECTRONIC:

Department of Defense Deployment Health Support Directorate. "Depleted Uranium Information Page." 2001. <[http://www.deploymentlink.osd.mil/du\\_library/](http://www.deploymentlink.osd.mil/du_library/)> (March 6, 2003).

International Committee of the Red Cross. "Depleted Uranium Munitions." June 6, 2001. <<http://www.icrc.org/Web/eng/siteeng0.nsf/htmlall/57JR5D?OpenDocument>> (March 6, 2003).

---

## USAMRICD (United States Army Medical Research Institute of Chemical Defense)

---

The United States Army Medical Research Institute of Chemical Defense (USAMRICD) located in Aberdeen Proving Ground, Maryland, is a research and training laboratory dedicated to advancing the treatments that alleviate the suffering caused by chemical weapons and developing new materials that aid in those treatments. Researchers at the laboratory include experts in physiology, toxicology, pathology and biochemistry.

Established in 1922 as part of the Army Medical Department, the laboratory was responsible for treating chemical weapon casualties during World War I. In the 1960s the division was renamed the U.S. Army Biomedical Laboratory. The laboratory was put under the command of the U.S. Army Surgeon General in 1979 and received its



A research scientist processes anthrax samples that are thought to contain a significant aerosol and respiratory hazard. AP/WIDE WORLD PHOTOS.

current name in 1981. Today, the USAMRICD is one of six laboratories and institutes under the authority of the U.S. Army Medical Research and Materiel Command.

Researchers at the USAMRICD have made hundreds of contributions to the scientific literature and have produced technical bulletins on procedures for collecting, handling, shipping, and preparing samples of chemical agents. The laboratory also operates a chemical surety facility. Along with its research charge, the USAMRICD is also a training institution. The Chemical Casualty Care Division (CCCD) provides courses in the management and treatment of chemical weapons injuries to medical professionals. Courses are offered at the laboratory, at off-site locations and as computer-based training. Much of the educational and training work of the USAMRICD is done in partnership with the United States Army Medical Research Institute of Infectious Disease (USAMRIID) in Fort Detrick, Maryland, which is the Army's primary laboratory for research into biological warfare agents.

#### ■ FURTHER READING:

##### ELECTRONIC:

United States Army <<http://mrmc-www.army.mil/>> ( April 10, 2003).

United States Army Medical Research Institute of Chemical Defense <<http://chemdef.apgea.army.mil/>> (April 10, 2003).

#### SEE ALSO

*Chemical Warfare*

*USAMRIID (United States Army Medical Research Institute of Infectious Diseases)*

## USAMRIID (United States Army Medical Research Institute of Infectious Diseases)

■ BRIAN HOYLE

USAMRIID is an acronym for the United States Army Medical Research Institute of Infectious Diseases. The facility is operated by the Department of Defense and serves as the country's principal laboratory for research into the medical aspects of biological warfare. Specifically, the facility aims to develop vaccines for infectious

diseases, other treatments such as drugs, and tests to detect and identify disease-causing microorganisms.

While developed for use in the laboratory, USAMRIID is mandated to explore the use of the treatments and tests in the real world of the battlefield. The research conducted at USAMRIID is defensive in nature. Infectious microbes are investigated only to develop means of protecting soldiers from the use of the microbes by opposition forces during a conflict.

The infectious disease research expertise at USAMRIID is also utilized to develop strategies and training programs to do with medical defense against infectious microorganisms. For example, the agency regularly updates and publishes a handbook that details the various medical defenses against biological warfare or terrorism. This handbook, now in its fourth edition, is available to the public.

While some of the research conducted at USAMRIID is classified, other research findings of the resident civilian and military scientists are used to benefit the larger public community. USAMRIID and its counterpart USAMRICD (U.S. Army Medical Research Institute of Chemical Diseases) trains more than 550 military medical personnel each year on biological and chemical defense measures. Furthermore, over 40,000 military and civilian medical professionals have attended an annual course on the Medical Management of Biological Casualties from 1999 to 2002.

**History of the USAMRIID.** The Office of the Surgeon General of the Army established USAMRIID on January 27, 1969. The facility replaced the U.S. Army Medical Unit (USAMU), which had been operating at the Fort Detrick, Maryland location since 1956. The USAMU had a mandate to conduct research into the offensive use of biological and chemical weapons. This research was stopped by U.S. President Richard Nixon in 1969. In 1971 and 1972, the stockpiled biological weapons were destroyed.

The defensive research that USAMU had been conducting, such as vaccine development, was continued by USAMRIID. In 1971, the facility was reassigned to the U.S. Army Medical Research and Development Command. Also in 1971, the centerpiece laboratory was completed. Construction of the high laboratory, which was designed to house and study highly infectious and dangerous microorganisms, cost \$14 million.

**Biocontainment capability.** Laboratories have a rating system with respect to the types of microbes that can safely be studied. There are four levels possible. A typical university research lab with no specialized safety features (i.e., fume hood, biological safety cabinet, filtering of exhausted air) is a Biosafety Level 1. Progression to a higher level requires more stringent safety and biological controls. A Biosafety Level 4 laboratory is the only laboratory that can safely handle microbes such as the Ebola virus, *Bacillus*

*anthracis* (the cause of anthrax), the Marburg virus, and hantavirus.

USAMRIID has a 10,000 square foot Biosafety Level 4 facility and 50,000 square feet of Biosafety Level 3. It is the largest high-level containment facility in the United States and is one of only three such units. The others are at the Centers for Disease Control and Prevention in Atlanta, Georgia, and San Antonio, Texas. A fourth level 4 laboratory is planned for the Rocky Mountain Lab in Hamilton, Montana.

Entry to the Level 4 area requires passage through several checkpoints and the keying in of a security code that is issued only after the person has been successfully vaccinated against the microorganism under study. All work in the level 4 lab is conducted in a pressurized and ventilated suit. Air for breathing is passed into the suit through a hose and is filtered so as to be free of microorganisms.

The USAMRIID facility also contains a Biosafety Level 4 patent ward. The ward can house people who have been infected during a disease outbreak or researchers who have been accidentally exposed to an infectious microbe. This ward was used in 1982 to care for two researchers from the Centers for Disease Control and Prevention who were exposed to rat blood contaminated with the virus that causes Lassa fever. The two researchers, along with three others thought to have been exposed to the virus remained in the containment ward until they were determined to be free of infection.

Equipment is also available that allows the Biosafety Level 4 conditions to be mimicked in the field. Thus, an infected person can be isolated at the site of an outbreak and transported back to Fort Detrick for medical treatment and study of the infection.

**Research and other activities.** The research staff at USAMRIID numbers over 500 people and includes physicians, microbiologists, molecular biologists, virologists, pathologists, and veterinarians. Among the support staff who assist the researchers are laboratory technicians who have volunteered to be test subjects during clinical trials of vaccines and drugs.

As of late 2002, USAMRIID scientists have the ability to rapidly identify approximately 85 infectious microorganisms. Work is underway to develop protection against 40 of the microbes. Vaccines are in various stages of development for 10 of the microbes including the highly infectious anthrax bacterium, and the Ebola and Marburg viruses.

Researchers and support staff can also respond to disease outbreaks. On short notice, teams can journey to the site of the infection to begin an investigation. This response is often conducted in conjunction with personnel from the Centers for Disease Control and Prevention. USAMRIID teams can also respond to combat. A portable laboratory to treat biological warfare casualties can be quickly set up near a battlefield.



One well-known USAMRIID response occurred in 1989, when an outbreak of an Ebola virus occurred at a primate holding facility in nearby Reston, Virginia. Some personnel even became infected with the virus, which was later determined to be a different variety from that which causes hemorrhagic Ebola fever in humans. The response of the USAMRIID personnel was subsequently detailed in best-selling books and inspired popular movies.

The facility has played an important role in several military campaigns. For example, it served as the medical support staging area for vaccines, drugs, and medical equipment during Operation Desert Storm and Desert Shield beginning in October 1990. During these campaigns, the threat of biological warfare, including the use of anthrax and *Clostridium botulinum* spores, was real. USAMRIID's expertise in treating these infections was invaluable to the troops who were sent to Saudi Arabia and Kuwait.

**USAMRIID and domestic terrorism.** In the aftermath of the September 11, 2001 terrorist attacks on targets in the United States, several letters containing anthrax spores were sent to various locations in the eastern United States via the United States Postal Service. The culprits have not been apprehended as of late 2002. Sequencing of the genetic material from the spores determined that the source of the anthrax was a strain of the microbe that had been developed in the USAMRIID labs in the 1980s. Whether the bacteria actually used in the incidents came from USAMRIID or from another lab that acquired the bacteria from USAMRIID has not been established.

Between September 11 and the following May, USAMRIID received 31,000 samples, an average of almost 4,000 per month, and performed over 260,000 tests. During normal times four to six samples are analyzed each month. Before September 11, the Special Pathogens Sample Test Laboratory had a staff of six. Since the crisis, a tenfold increase in staff members work around the clock.

#### ■ FURTHER READING:

##### BOOKS:

USAMRIID *USAMRIID's Medical Management of Biological Casualties Handbook, Fourth Edition*. Fort Detrick, MD: U.S. Army Medical Research Institute of Infectious Diseases, 2001.

##### ELECTRONIC:

USAMRIID. "Welcome to USAMRIID." The U.S. Army Medical Research Institute of Infectious Diseases. Fort Detrick, MD. July 25, 2002. <<http://www.usamriid.army.mil/>>(25 November 2002).

##### SEE ALSO

*Biocontainment Laboratories*  
*Biological Weapons, Genetic Identification*  
*United States, Counter-terrorism Policy*  
*Vaccines*

## USS Cole

■ STEPHANIE WATSON

On the morning of October 12, 2000, as the Navy destroyer USS *Cole* sat anchored in the Yemeni port of Aden, a small boat packed with explosives rammed into its side, tearing a 40-foot hole through the ship's outer hull, killing seventeen sailors and wounding thirty-nine more. It was the deadliest attack against the United States military since 1996, when a truck bomb exploded near an apartment complex in Dhahran, Saudi Arabia, killing 19 American servicemen.

**A ship in hostile waters.** The *Cole*, one of the Arleigh Burke class of guided missile destroyers, was based in Norfolk, Virginia. The ship was on its way from the Red Sea to the Persian Gulf to help enforce United Nations sanctions against Iraq, when it made a routine stop in the Yemeni port of Aden for refueling. American intelligence officials had long been aware that Yemen was home to a number of Islamist fundamentalist groups. In the weeks before the attack, the country was home to violent demonstrations against the treatment of Palestinians in the Israeli-Palestinian conflict and America's supposed pro-Israeli stance. Although *Cole* Commander Kirk Lippold had been told of no specific threat against his ship, it was on what is known as "Threat Condition Bravo"—the second highest of four threat levels. At alerts of that level, the ship's guards were required to be on the lookout for small boats.

No flags were apparently raised when a small fiberglass boat approached the *Cole*. Eyewitnesses said the boat was helping the big destroyer with its mooring, when it pulled back to the *Cole's* port side. The two men on board reportedly stood at attention before their boat exploded, blowing a massive hole in the destroyer's steel hull. Damage to the \$1 billion warship was estimated at \$250 million.

Within hours of the explosion, Pentagon officials said they had reason to suspect a terrorist attack. FBI and CIA agents, as well as the Pentagon's Fleet Anti-Terrorist Support Team, were quickly sent to the scene to investigate. Within weeks, officials announced that they believed the blast to be the work of Osama bin Laden, the Saudi Arabian exile whose al-Qaeda terrorist network was also connected to the 1998 bombings of two American embassies in Kenya and the 1993 World Trade Center bombing. Al-Qaeda would later be linked to the September 11, 2001 attacks on the World Trade Center and Pentagon.

As the FBI and CIA began piecing together the evidence, they revealed that this wasn't the first plot against U.S. military interests in the region. Intelligence officials said they had already foiled at least two attempted plots against American ships. In mid-September 2000, a CIA report indicated the possibility that terrorists would attack a warship in the Mediterranean using a boat filled with



United States Navy and Marine Corps security personnel patrol past the damaged destroyer USS *Cole* following the October 12, 2000, terrorist bombing attack on the ship in Aden, Yemen. ©AFP/CORBIS.

explosives. And just two weeks before the attack, the Arab news channel Al Jazeera broadcast a video of bin Laden in which he made threats against the United States.

**A troubled investigation.** Although American intelligence officials moved quickly after the USS *Cole* attack, the investigation hit a number of snags. Yemeni officials questioned more than 1,500 people, yet they restricted American officials' access to key suspects. In June 2001, FBI agents were pulled out of Yemen because of credible evidence that there was a terrorist threat against them. The FBI and U.S. State Department disagreed over how to steer the investigation and deal with the uncooperative Yemeni government. The U.S. government still could not prove that al-Qaeda was behind the attack, and they were concerned that several key operatives remained at large, possibly planning more attacks against American interests.

United States officials did make significant progress in their investigation, eventually capturing several key suspects in the attack. In October 2002, the FBI nabbed a senior al-Qaeda operative named Abd Al-Rahim al-Nashiri, who is suspected of masterminding the *Cole* attack, as well as plotting several other attacks against other U.S. and British warships. The following month, a CIA-launched

missile killed Abu Ali (also known as Qaed Senyan), a man who was said to have played a major role in the *Cole* attack, as he was traveling with five other al-Qaeda members in Yemen.

#### ■ FURTHER READING:

##### PERIODICALS:

Hosenball, Mark, and Greg Vistica. "The Search for Clues: Did Officials Miss Hints of an Impending Attack?" *Newsweek*. November 6, 2000:45.

Kaplan, David E., Chitra Ragavan, and Richard J. Newman, et al. "Terror's Grim Toll." *U.S. News & World Report*. October 30, 2000:32.

MacLeod, Scott, Elaine Shannon, Mark Thompson, Edward Barnes, and William Dowell. "How Feuds and Culture Clashes Have Stymied the USS *Cole* Investigation." *Time*. Volume 158 (July 16, 2001): 38.

Nordland, Rod, John Barry, Mark Hosenball, Debra Rosenberg, and Gregory Vistica. "A Sneak Attack: Death at Sea." *Newsweek*. October 23, 2000: 27.

##### ELECTRONIC:

U.S. Department of State. "Attack on the USS *Cole*: IIP Archives." <<http://usinfo.state.gov/topical/pol/terror/colearch.htm>> (December 20, 2002).

## SEE ALSO

FBI (United States Federal Bureau of Investigation)  
Port Security

USS *Lapon*.

SEE *Undersea Espionage: Nuclear vs. Fast Attack Subs.*

---

## USS *Liberty*

---

■ ADRIENNE WILMOTH LERNER

The Liberty Incident refers to the June 8, 1967, attack on the United States intelligence ship *Liberty* by Israeli Defense Forces. The *Liberty* was stationed near the Sinai Peninsula and charged with monitoring Soviet communications to Soviet Arab allies during the Arab-Israeli Six Day War. Israeli troops reported they were taking fire from warships and deployed aircraft to find the source of enemy fire. The planes found the *Liberty* and fired upon the vessel. Torpedo boats also seized upon the *Liberty*. The attack killed 34 Americans, wounded 171, and destroyed the American ship. Israeli forces claimed that they had misidentified the *Liberty* as a hostile ship and attacked the vessel in error. Although the event sparked controversy, the attack was soon ruled an accident.

The USS *Liberty* was a World War II-era freighter built in 1945. The vessel sailed in post-war operations in the Pacific until it was retired in 1958. At the height of Cold War tensions, the National Security Agency (NSA) refitted several older military ships, turning them into intelligence vessels. The Liberty-class ships were designed to track radio signals and monitor communications between the Soviet Union and its allies. The *Liberty* itself measured over 450 feet long and carried a crew of 290 military and intelligence personnel.

The *Liberty*, like other ships in the intelligence fleet, was not constructed to be a warship. Navy and NSA officials assessed the risk of the ships encountering hostile forces was minimal, since all were to conduct operations only in international waters. The *Liberty* carried minimal defensive weapons, with only four .50 caliber machine guns mounted on the ship's deck. While the vessel was marked with its U.S. Navy identification number and flew an American flag, the ship maintained radio silence during most of its operations. Since the ships conducted operations in international waters, the American Navy rarely reported the position of its intelligence vessels to foreign intelligence services. Despite mission secrecy, the *Liberty's* national origin and electronic surveillance capabilities could be ascertained by trained, careful observers.

The *Liberty's* first mission as a refitted intelligence ship was monitoring radio communications off the coast of West Africa. As tensions grew between Israel and neighboring Arab nations, the *Liberty* was deployed to the eastern Mediterranean Sea. The vessel took on new personnel, including technical specialists and linguists trained in Russian and Arabic. However, no specially trained Hebrew language experts were assigned to the *Liberty*. The *Liberty* was stationed 13 miles off the Gaza coast, precariously close to Israel and Egypt, and in the middle of the developing conflict in the Middle East.

The presence of Soviet bombers in Alexandria strained U.S. relations with Egypt. As a result, diplomatic friendliness between Israel and the United States increased in an effort to halt Soviet backing of various Middle Eastern governments with military aid. The USS *Liberty's* mission was to conduct remote intelligence, listening to radio transmissions, to ascertain the status of Soviet bombers and military officers in Egypt. As the ship began its mission, the Six-Day War erupted. Commander William McGonagle, Captain of the USS *Liberty*, requested a destroyer escort for his vessel, but the request was denied. Instead, U.S. Naval Command told McGonagle that jet fighter squadrons stationed on the island of Crete could provide rapid assistance if needed. A few hours later, U.S. Naval Command issued new orders to the *Liberty* to retreat further into international waters, 25 miles from the Sinai Peninsula. The *Liberty* never received the revised orders.

The *Liberty* remained in its location. Assured that the new orders had been received and heeded by the crew, U.S. military forces assured allies in the United Nations that no American vessels were present in the war area. On June 8, 1967, Israeli troops reported that they were being fired on from vessels at sea. Israeli intelligence deployed jet fighters to scout for Egyptian and other hostile boats in the region. Jet fighter scouts mistakenly reported to Israeli Defense Force Command that they located the Egyptian vessel, *El Quseir*, which had attacked Israel forces the day before. However, the planes actually reported the location of the USS *Liberty*, which they had misidentified.

Israeli forces swiftly attacked the *Liberty* with both jet fighters. The *Liberty* responded by turning its only weapons, the four .50 caliber machine guns, on the assaulting forces. The Israelis responded by launching napalm canisters and torpedoes from warships. The *Liberty* broke radio silence and tried to contact Israeli forces to identify the vessel as an American intelligence ship. However, Israeli forces had jammed the ship's communications systems with extensive static. Finding an open channel, *Liberty* communications officers radioed U.S. air forces in Crete for assistance. Receiving the distress call, jet fighters were deployed to aid the besieged *Liberty*. However, U.S. military officials recalled the planes after discovering that the jet fighters were not equipped to repel the attack. Without defensive weapons or fighting assistance, the *Liberty* was quickly crippled. Crewmembers later reported that Israeli



Israeli planes and one or more torpedo boats mistakenly attacked this U.S. Navy research ship, the USS *Liberty*, in the Mediterranean Sea near the Sinai Peninsula in 1967. ©BETTMANN/CORBIS.

forces opened machine gun fire on men trying to escape the flaming wreckage. Radio operators onboard the American ship finally sent a successful communication to Israeli forces, identifying the *Liberty*.

The barrage ceased, and Israeli forces notified government and intelligence officials, that they had mistakenly fired upon an American vessel. The Israeli government reported the incident immediately to the United States embassy in Tel Aviv, and notified U.S. officials in Washington, D.C. United States Naval Command deployed nearby ships in a belated rescue effort. Before U.S. aid vessels arrived, Israeli and Soviet vessels in the area both offered assistance to the crew of the *Liberty*. McGonagle and his crew refused their aid.

Though the incident was shrouded in secrecy for numerous years, the U.S. government declassified most of the documents surrounding the Israeli attack on the *Liberty* in the mid 1990s. Though some people, including various crewmembers, remain skeptical about the motive and nature of Israeli military actions against the ship, the Liberty Incident was officially ruled a "friendly fire" accident. Volumes of documents and diplomatic evidence materials support this conclusion.

In July 1967, the U.S. Navy conducted the first official investigation of the Liberty Incident. The investigation team collaborated Israeli accounts that the ship was hastily misidentified as result of wartime stresses on military and intelligence resources. The inquiry noted relatively calm seas prevented the ship's flags from visible flight, and that jammed radios onboard the ship hampered communication. Furthermore, the Navy acknowledged that officials did not report the position of the USS *Liberty* to Israeli intelligence. Twelve subsequent, individual investigations, nine by the United States government and three by Israeli officials, concluded that the attack on the *Liberty* was the result of error. Israel officially apologized for the incident on several occasions, and paid \$13 million in reparations. Despite the incident, the United States and Israel maintained increasingly good diplomatic relations. On December 17, 1987, the two governments formally closed diplomatic discussions on the incident.

The USS *Liberty* was not the only Liberty-class intelligence vessel involved in an international incident. The *Liberty's* sister ship, the USS *Pueblo* was seized by North Korean forces while conducting surveillance missions in international waters off the Korean Peninsula.

## ■ FURTHER READING:

### BOOKS:

Gerhard, William D. *Attack on the USS Liberty*. Laguna Hills, CA: Aegean Park, 1996.

Cristol, A. Jay. *The Liberty Incident: The 1967 Attack on the U.S. Navy Spy Ship*. Washington, D.C.: Brassey's Military, 2002.

### SEE ALSO

*Israel, Intelligence and Security*  
*Pueblo Incident*  
*Radio, Direction Finding Equipment*

---

## USSTRATCOM (United States Strategic Command)

---

United States Strategic Command, or USSTRATCOM, was formed by a 2002 merger between the Air Force Strategic Command and the U.S. Space Command. Located at Offutt Air Force Base in Nebraska, USSTRATCOM is one of nine unified commands in the Department of Defense. It serves as the command and control center for U.S. strategic forces, as well as military space operations, including the operation of military satellites. In its function as a strategic command center, it is responsible both for early warning against missile attack, as well as the launch of missiles in response.

The Strategic Command portion of USSTRATCOM had its beginnings in March 1946, with the establishment of the U.S. Air Force Strategic Air Command (SAC) at Offutt. At the height of the Cold War, Offutt was the command center for the defense "triad": the strategic bombers and ICBMs (intercontinental ballistic missiles) of the Air Force, and the U.S. Navy's submarine-launched ballistic missiles. On June 1, 1992, with the Cold War over, SAC and the Navy's Joint Strategic Target Planning Staff merged as the U.S. Strategic Command. Thenceforth, all planning, targeting, and wartime deployment of strategic forces would be under a single command, while the day-to-day operations remained with the respective services.

The U.S. Space Command had its roots in the military launches that began in the wake of the Soviets' deployment of the *Sputnik* satellite in 1957. The most visible portions of the space program were the Pioneer and Apollo programs, but Army, Navy, and Air Force activities in space continued throughout the 1960s, 1970s, and 1980s. In September 1985, the Joint Chiefs of Staff created the U.S. Space Command to unify these efforts. During the Persian Gulf War and other military engagements of the 1990s, satellites under the Space Command assisted in surveillance, reconnaissance, and targeting.

USSTRATCOM, established on October 1, 2002, is responsible both for early warning and defense against missile attack and long-range conventional attacks. It is also charged with deterring and defending against the proliferation of weapons of mass destruction. Some 2,500 personnel, representing all four services, along with Department of Defense civilians and contractors, work at the command center. Located in the Underground Command Complex at Offutt, a two-level, 14,000-square-foot (1,301 square mile) reinforced concrete and steel structure, the Command Center is housed alongside the Intelligence Operations Center, Weather Support Center, Force Status Readiness Center, and other support offices.

## ■ FURTHER READING:

### PERIODICALS:

Clinton, William J. "Remarks on Arrival at Offutt Air Force Base in Bellevue, Nebraska." *Weekly Compilation of Presidential Documents* 36, no. 50 (December 18, 2000): 3041.

Garth, Jeff. "Retired General to Oversee Nuclear Weapons Labs." *New York Times*. (June 17, 1999): A15.

Gordon, Michael R. "U.S. Arsenal: Treaties vs. Nontreaties." *New York Times*. (November 14, 2001): A12.

Myers, Steven Lee. "U.S. 'Updates' All-Out Atom War Guidelines." *New York Times*. (December 8, 1997): A3.

### ELECTRONIC:

United States Strategic Command. <<http://www.stratcom.af.mil/>> (March 28, 2003).

### SEE ALSO

*Ballistic Missiles*  
*DoD (United States Department of Defense)*  
*Nuclear Weapons*  
*Satellites, Spy*



---

## Vaccination

---

United States President George W. Bush authorized a program on December 13, 2002, which by its conclusion, will see approximately 500,000 military personnel vaccinated against smallpox, along with an equal number of key healthcare providers in the United States. In the event of a biological attack that would expose Americans to smallpox, the affected citizens could then be quickly vaccinated by the protected healthcare workers. Additionally, the vaccine will be offered to up to ten million police, firefighters, and other first responders to emergencies. Smallpox vaccination within three days of exposure will usually prevent development of the disease, or dramatically reduce its virulence. Plentiful stocks are on hand in the U.S. to respond to a large smallpox outbreak, and vaccine in quantities necessary for inoculation of the entire population of the United States are in production. By mid-2004, health officials plan to have smallpox vaccinations available on a voluntary basis for all Americans.

An anthrax vaccine is also available and is only routinely given to laboratory workers who are involved with *B. anthracis* study or cultures. Vaccination for anthrax prevention involves a series of six injections over an 18-month period. Over 500,000 military personnel received the vaccine as a precaution in 2002, but for the general population, including medical providers and first responders, the vaccine is not currently recommended as other options such as antibiotic treatment offer protection to individuals exposed to anthrax-causing bacteria.

Diseases like anthrax and smallpox are among those microbial diseases that could be exploited as biological weapons. Indeed, anthrax was sent through the postal system to targets in the United States in the aftermath of the September 11, 2001 terrorist attacks in the U.S. Anthrax is a disease caused by the bacterium *Bacillus anthracis*, which can infect the skin, digestive tract, or lungs. Lung

infection is often fatal. Smallpox is an extremely contagious disease that is caused by the variola virus.

Vaccination refers to the procedure in which the presence of a component of a microorganism such as a protein (the antigen) stimulates the defense mechanism of the host, which is known as the immune system, to form an antibody. Each antibody is formed in specific response to a particular antigen. The antibodies act to protect the host from future exposure to the antigen (immunity). Depending on the disease and the nature of the vaccine, the immunity can last from a year or two (i.e., influenza) to a lifetime.

Vaccination is protective against infection without the need of suffering through a bout of a disease. In this artificial process an individual receives the antibody-stimulating compound either by injection or orally. Some vaccines like that for smallpox do contain live microorganisms, which can cause some discomfort and, in rare cases, more serious complications. Nonetheless, for most people, vaccination is a prudent step to avoid the threat of a disease. As of early 2003, only one healthcare worker having received the recent smallpox vaccine reported a related complication, a non-life threatening vaccinia rash. Less than a dozen instances of complication (none considered serious) have been reported among military personnel receiving the vaccine.

The technique of vaccination has been practiced since at least the early decades of the eighteenth century. Then, a common practice in Istanbul, Turkey was to retrieve material from the surface sores of a smallpox sufferer and rub the material into a cut on another person. The recipient was often spared the ravages of smallpox. This practice was noted by Lady Mary Wortley Montague, the wife of the British Ambassador Extraordinary to the Turkish court. Upon her return to England, she used her social standing to promote the benefits of this crude method of smallpox inoculation. Among those who were convinced was the Royal Family. Indeed, it became fashionable to receive an inoculation, partly perhaps it carried social

cache. The technique was refined by Edward Jenner into a vaccine for cowpox in 1796.

Since Jenner's time, vaccines for a variety of bacterial and viral maladies have been developed. The material used for vaccination is one of four types. Some vaccines consist of living but weakened viruses. Such an attenuated vaccine does not cause an infection but does elicit an immune response. An example is the measles, mumps, and rubella (MMR) vaccine. The second type of vaccine can involve killed viruses or bacteria. The virus or bacteria need to be killed in a way that does not perturb their surfaces. This care is necessary to preserve the three-dimensional structure of surface molecules that stimulate the immune response. Agents such as alum can be used to enhance the immune response to the killed target, perhaps by exposing the antigen to the immune system for a longer time. A third type of vaccination involves a toxoid, which is an inactivated form of a toxin produced by the target bacterium. Examples of toxoid vaccines are the diphtheria and tetanus vaccines. Lastly, a biosynthetic vaccine can utilize a synthetic compound pieced together from portions of two antigens. The Hib vaccine is a biosynthetic vaccine.

Vaccinations against some diseases occurs early in life. For example, during an infant's first two years of life, a series of vaccinations is recommended to develop protection against hepatitis B, polio, measles, mumps, rubella (also called German measles), pertussis (also called whooping cough), diphtheriae, tetanus (lockjaw), *Haemophilus influenzae* type b, pneumococcal infections, and chickenpox. Multiple injections of the vaccine can be required to ensure that the immunity that develops is long lasting. For example, vaccination against diphtheria, tetanus, and pertussis is typically administered at 2 months of age, 4 months, 6 months, 15 to 18 months, and finally at 4 to 6 years of age.

A series of vaccinations such as the above triggers a greater production of antibody by the immune system.

The immune cells that respond to the presence of an antigen in a vaccine are called lymphocytes. Prior to vaccination there are a multitude of lymphocytes, each of which recognizes a single specific protein or a portion of the protein. The presence of a specific antigen stimulates that lymphocyte that recognizes the antigenic target. That lymphocyte will then divide repeatedly and the daughter cells will produce antibody. Eventually, there are many daughter lymphocytes and a lot of antibody circulating in the body.

If the antigen does not persist in the body, the production of antibodies will stop. But the lymphocytes that have been produced still retain the memory of the target protein. When the target is presented again to the lymphocytes, as happens in the second vaccination in a series, the many lymphocytes are stimulated to divide into daughter cells, which in turn form antibodies. This is because the immune cells that responded to the antigen upon the first exposure "remember" the antigen, and so can produce

even more antibody when presented with the antigen a second or third time. In immunological terms the immune cells are said to be "primed." This form of antigenic memory can last for a lifetime for diseases such as diphtheria and pertussis. For other diseases such as tetanus adults should be vaccinated every ten years (a "booster shot") in order to keep their bodies primed to fight the tetanus microorganism.

Many vaccinations are given via injection. However, solutions that can be drunk are also used. The classic example is the oral vaccine to polio devised by Albert Sabin. Oral vaccination is often limited by the passage of the vaccine through the highly acidic stomach. In the future is hoped that the bundling of the vaccine in a protective casing will prevent the damage caused in the stomach. Experiments using bags made out of lipid molecules (liposomes) has demonstrated both protection of the vaccine and the ability to tailor the liposome release of the vaccine.

While the benefits of vaccination are obvious, this protection against disease does not come without a risk. For a variety of vaccines, side effects are possible. For some vaccines, the side effects are minor. A person may, for example, develop a slight ache and redness at the site of injection. In some very rare cases, however, more severe reactions can occur, such as convulsions and high fever. The smallpox vaccine carries the risk of encephalitis (swelling of cells of the brain and spinal cord) in approximately three to 12 people per million people vaccinated.

#### ■ FURTHER READING:

##### BOOKS:

- Joellenbeck, Lois M., Lee L. Zwanziger, Jane S. Durch, and Brian L. Strom. *The Anthrax Vaccine: Is It Safe? Does It Work?* Washington: Joseph Henry Press, 2002.
- Murphy, Christine. *The Vaccine Dilemma*. New York: Lantern Books, 2000.
- Neustaedter, Randall. *The Vaccine Guide: Risks and Benefits for Children and Adults*. Berkeley: North Atlantic Books, 2002.

##### ELECTRONIC:

- Centers for Disease Control and Prevention. "Vaccine Fact Sheets." National Vaccine Program Office. November 23, 2002. <[http://www.cdc.gov/od/nvpo/fs\\_toc.htm](http://www.cdc.gov/od/nvpo/fs_toc.htm)>(6 January 2003).

##### SEE ALSO

*Biocontainment Laboratories*  
*Biological Warfare*  
*Pathogens*

## Vaccine Event Reporting System.

SEE *Anthrax Vaccine*.

# Vaccines

■ JULI BERWALD

A vaccine is a medical preparation given to a person to provide immunity from a disease. Vaccines use a variety of different substances ranging from dead microorganisms to genetically engineered antigens to defend the body against potentially harmful antigens. Effective vaccines change the immune system by promoting the development of antibodies that can quickly and effectively attack disease causing microorganisms or viruses when they enter the body, preventing disease development.

## Vaccine Development

The development of vaccines against diseases including polio, smallpox, tetanus, and measles is considered among one of the great accomplishments of medical science. Researchers are continually attempting to develop new vaccinations against other diseases. In particular, vigorous research into vaccines for Acquired Immune Deficiency Syndrome (AIDS), cancer and Severe Acute Respiratory Syndrome (SARS) is currently underway.

The first successful vaccine was developed from cowpox as a treatment for smallpox. Coined by Louis Pasteur (1822–1895), the etymology of the term vaccine reflects this achievement. It is taken from the Latin for cow (*vacca*) and the word vaccinia, the virus that causes cowpox.

**Smallpox.** The first effective vaccine developed treated smallpox, a virulent disease that killed thousands of its victims and left thousands of others disfigured. In one of the first forms of inoculation, the ancient Chinese developed a snuff made from powdered smallpox scabs that was blown into the nostrils of uninfected individuals. Some individuals died from the therapy; however, in most cases, the mild infection produced offered protection from later, more serious infection.

In the late 1600s, European peasants employed a similar method of immunizing themselves against smallpox. In a practice referred to as “buying the smallpox,” peasants in Poland, Scotland, and Denmark reportedly injected the smallpox virus under the skin to obtain immunity.

Lady Mary Wortley Montague, the wife of the British ambassador to Turkey brought information on immunization back to Europe in the early 1700s. Montague reported that the Turks injected a preparation of smallpox scabs into the veins of susceptible individuals. Those injected generally developed a mild case of smallpox from which they recovered rapidly. Montague convinced King George I to allow trials of the technique on inmates in Newgate

Prison. Although some individuals died after receiving the injections, the trials were successful enough that variolation, or the direct injection of smallpox, became accepted medical practice. Variolation also was credited with protecting United States soldiers from smallpox during the Revolutionary War.

Edward Jenner (1749–1823), an English country physician, observed that people who were in contact with cows often developed cowpox, which caused pox sores but was not life threatening. Those people never developed smallpox. In 1796, Jenner tested the hypothesis that cowpox could be used to protect humans against smallpox. He injected a healthy eight-year-old boy with cowpox obtained from a milkmaid’s sore. The boy was moderately ill and recovered. Jenner then injected the boy twice with the smallpox virus, and the boy did not get sick.

Modern knowledge of the immune system suggests that the virus that causes cowpox is similar enough to the virus that causes smallpox that the vaccine simulated an immune response to smallpox. Exposure to cowpox antigen stimulated the boy’s immune system, producing cells that attacked the original antigen as well as the smallpox antigen. The vaccine also conditioned the immune system to produce antibodies more quickly and more efficiently against future infection by smallpox.

During the two centuries since its development, the smallpox vaccine gained popularity, protecting millions from contracting the disease. In 1979, following a major cooperative effort between nations and several international organizations, world health authorities declared smallpox the only infectious disease to be eradicated from the planet.

**Rabies.** In 1885 Louis Pasteur (1822–1895) saved the life of Joseph Meister, a nine year old who had been attacked by a rabid dog. Pasteur’s series of experimental rabies vaccinations on the boy proved the effectiveness of the new vaccine.

Pasteur’s rabies vaccine, the first human vaccine created in a laboratory, was made of an extract gathered from the spinal cords of rabies-infected rabbits. The live virus was weakened by drying over potash. The new vaccination was far from perfect, causing occasional fatalities and temporary paralysis. Individuals had to be injected 14 to 21 times.

The rabies vaccine has been refined many times. In the 1950s, a vaccine grown in duck embryos replaced the use of live virus, and in 1980, a vaccine developed in cultured human cells was produced. In 1998, the newest vaccine technology—genetically engineered vaccines—was applied to rabies. The new DNA vaccine cost a fraction of the regular vaccine. While only a few people die of rabies each year in the United States, more than 40,000 die worldwide, particularly in Asia and Africa. The less expensive vaccine will make vaccination far more available to people in less developed nations.



**Polio.** In the early 1900s polio was extremely virulent in the United States. At the peak of the epidemic, in 1952, polio killed 3,000 Americans, and 58,000 new cases of polio were reported.

In 1955 Jonas Salk (1914–1995) developed a vaccine for poliomyelitis. The Salk vaccine, a killed virus type, contained the three types of poliovirus that had been identified in the 1940s. In the first year the vaccine was distributed, dozens of cases of polio were reported in individuals who had received the vaccine or had contact with individuals who had been vaccinated. This resulted from an impure batch of vaccine that had not been completely inactivated. By the end of the incident, more than 200 cases had developed and 11 people had died.

In 1961, an oral polio vaccine developed by Albert B. Sabin (1906–1993) was licensed in the United States. The Sabin vaccine, which uses weakened, live polio viruses, quickly overtook the Salk vaccine in popularity in the United States, and is currently administered to all healthy children. Because it is taken orally, the Sabin vaccine is more convenient and less expensive to administer than the Salk vaccine.

Advocates of the Salk vaccine, which is still used extensively in Canada and many other countries, contend that it is safer than the Sabin oral vaccine. No individuals have developed polio from the Salk vaccine since the 1955 incident. In contrast, the Sabin vaccine has a very small but significant rate of complications, including the development of polio. However, there has not been one new case of polio in the United States since 1975, or in the Western Hemisphere since 1991. Though polio has not been completely eradicated, there were only 144 confirmed cases worldwide in 1999.

**Influenza.** Developing a vaccine against the influenza virus is problematic because the viruses that cause the flu constantly evolve. Scientists grapple with predicting what particular influenza strain will predominate in a given year. When the prediction is accurate, the vaccine is effective. When they are not, the vaccine is often of little help. However, the flu shot has had enough success that pediatricians are now recommending the vaccine for children older than 6 months.

## AIDS Vaccine Research

Since the emergence of AIDS in the early 1980s, research for a treatment for the disease has resulted in clinical trials for more than 25 experimental vaccines. These range from whole-inactivated viruses to genetically engineered types. Some have focused on a therapeutic approach to help infected individuals to fend off further illness by stimulating components of the immune system; others have genetically engineered a protein on the surface of HIV to prompt immune response against the virus; and yet others attempted to protect uninfected individuals. The challenges in developing a protective vaccine include the fact

that HIV appears to have multiple viral strains and mutates quickly.

In January 1999, a promising study was reported in *Science* magazine of a new AIDS vaccine created by injecting a healthy cell with DNA from a protein in the AIDS virus that is involved in the infection process. This cell was then injected with genetic material from cells involved in the immune response. Once injected into the individual, this vaccine “catches the AIDS virus in the act,” exposing it to the immune system and triggering an immune response. This discovery offers considerable hope for development of an effective vaccine. As of April, 2003, a vaccine for AIDS had not been proven in clinical trials.

## Cancer Vaccine Research

Stimulating the immune system is considered key by many researchers seeking a vaccine for cancer. Currently numerous clinical trials for cancer vaccines are in progress, with researchers developing experimental vaccines against cancer of the breast, colon, and lung, among others. Promising studies of vaccines made from the patient’s own tumor cells and genetically engineered vaccines have been reported. Other experimental techniques attempt to penetrate the body in ways that could stimulate vigorous immune responses. These include using bacteria or viruses, both known to efficiently circulate through the body, as carriers of vaccine antigens. These bacteria or viruses could be treated or engineered to make them incapable of causing illness.

## Vaccine Production

The classic methods for producing vaccines use biological products obtained directly from a virus or a bacteria. Depending on the vaccination, the virus or bacteria is either used in a weakened form, as in the Sabin oral polio vaccine; killed, as in the Salk polio vaccine; or taken apart so that a piece of the microorganism can be used. For example, the vaccine for *Streptococcus pneumoniae*, which causes pneumonia, uses bacterial polysaccharides, carbohydrates found in bacteria which contain large numbers of monosaccharides, a simple sugar. The different methods for producing vaccines vary in safety and efficiency. In general, vaccines that use live bacterial or viral products are extremely effective when they work, but carry a greater risk of causing disease. This is most threatening to individuals whose immune systems are weakened, such as individuals with leukemia. Children with leukemia are advised not to take the oral polio vaccine because they are at greater risk of developing the disease. Vaccines which do not include a live virus or bacteria tend to be safer, but their protection may not be as great.

The classic types of vaccines are all limited in their dependence on biological products, which often must be kept cold, may have a limited life, and can be difficult to produce. The development of recombinant vaccines—those using chromosomal parts (or DNA) from a different

organism—has generated hope for a new generation of man-made vaccines. The hepatitis B vaccine, one of the first recombinant vaccines to be approved for human use, is made using recombinant yeast cells genetically engineered to include the gene coding for the hepatitis B antigen. Because the vaccine contains the antigen, it is capable of stimulating antibody production against hepatitis B without the risk that live hepatitis B vaccine carries by introducing the virus into the blood stream.

**DNA vaccines.** As medical knowledge has increased—particularly in the field of DNA vaccines—researchers are working towards developing new vaccines for cancer, melanoma, AIDS, influenza, and numerous others. Since 1980, many improved vaccines have been approved, including several genetically engineered (recombinant) types which first developed during an experiment in 1990. These recombinant vaccines involve the use of so-called “naked DNA.” Microscopic portions of a virus’s DNA are injected into the patient. The patient’s own cells then adopt that DNA, which is then duplicated when the cell divides, becoming part of each new cell. Researchers have reported success using this method in laboratory trials against influenza and malaria. These DNA vaccines work from inside the cell, not just from the cell’s surface, as other vaccines do, allowing a stronger cell-mediated fight against the disease. Also, because the influenza virus constantly changes its surface proteins, the immune system or vaccines cannot change quickly enough to fight each new strain. However, DNA vaccines work on a core protein, which researchers believe should not be affected by these surface changes.

**Vaccination programs.** The Children’s Vaccine Initiative, supported by the World Health Organization, the United Nations’ Children’s Fund, and other organizations, are working diligently to make vaccines easier to distribute in developing countries. More than four million people, mostly children, die every year from preventable diseases. Annually, measles kills 1.1 million children worldwide; whooping cough (pertussis) kills 350,000; hepatitis B 800,000; Haemophilus influenzae type b (Hib) 500,000; tetanus 500,000; rubella 300,000; and yellow fever 30,000. Another 8 million die from diseases for which vaccines are still being developed. These include pneumococcal pneumonia (1.2 million); acute respiratory virus infections (400,000), malaria (2 million); AIDS (2.3 million); and rotavirus (800,000). In August 1998, the Food and Drug Administration approved the first vaccine to prevent rotavirus—a severe diarrhea and vomiting infection.

Effective vaccines have limited many of the life-threatening infectious diseases. In the United States, children starting kindergarten are required to be immunized against polio, diphtheria, tetanus, and several other diseases. Other vaccinations are used only by populations at risk, individuals exposed to disease, or when exposure to a

disease is likely to occur due to travel to an area where the disease is common. These include influenza, yellow fever, typhoid, cholera, and Hepatitis A and B.

The measles epidemic of 1989 was a graphic display of the failure of many Americans to be properly immunized. A total of 18,000 people were infected, including 41 children who died after developing measles, an infectious, viral illness whose complications include pneumonia and encephalitis. The epidemic was particularly troubling because an effective, safe vaccine against measles has been widely distributed in the United States since the late 1960s. By 1991, the number of new measles cases had started to decrease, but health officials warned that measles remained a threat.

This outbreak reflected the limited reach of vaccination programs. Only 15% of the children between the ages of 16 and 59 months who developed measles between 1989 and 1991 had received the recommended measles vaccination. In many cases parents erroneously reasoned that they could avoid even the minimal risk of vaccine side effects “because all other children were vaccinated.”

Nearly all children are immunized properly by the time they start school. However, very young children are far less likely to receive the proper vaccinations. Problems behind the lack of immunization range from the limited health care received by many Americans to the increasing cost of vaccinations. Health experts also contend that keeping up with a vaccine schedule, which requires repeated visits, may be too challenging for Americans who do not have a regular doctor or health provider.

Internationally, the challenge of vaccinating large numbers of people has also proven to be immense. Also, the reluctance of some parents to vaccinate their children due to potential side effects has limited vaccination use. Parents in the United States and several European countries have balked at vaccinating their children with the pertussis vaccine due to the development of neurological complications in a small number of children given the vaccine. Because of incomplete immunization, whooping cough remains common in the United States, with 30,000 cases and about 25 deaths due to complications annually. One response to such concerns has been testing in the United States of a new pertussis vaccine that has fewer side effects.

**Vaccines against biological weapons.** The United States Centers for Disease Control have identified six diseases that are the most likely to be used in biological weapons. They are smallpox, anthrax, plague, botulism, tularemia and viral hemorrhagic fevers. Vaccines against these diseases are in various stages of development and dissemination.

After smallpox was eradicated from the United States in 1972, vaccination against the disease was discontinued. As a result, there are a substantial number of people in the United States that have never been exposed to the virus. A

majority of those vaccinated may have waning immunity because the smallpox vaccine provides a high level of immunity for approximately five years, with declining immunity thereafter. The United States has recently stockpiled enough vaccine to control an outbreak in case of a crisis, and plans are underway to increase vaccine production until stockpiles include enough vaccine to inoculate the entire U.S. population against smallpox.

Anthrax is of particular note as a biological weapon because it is an airborne pathogen that can be used in conjunction with traditional weapons. A vaccine against anthrax has recently been developed and it consists of a series of six subcutaneous injections. Because antibiotics are effective against the disease, the vaccine is currently only administered to populations at high risk, such as military personnel and researchers who handle the bacterium that causes anthrax.

Tularemia is caused by the bacterium *Francisella tularensis*, which is an extremely infectious airborne pathogen. Tularemia is usually treated with antibiotics, but a vaccine has been developed and the Food and Drug Administration is currently testing it. To date the vaccine has only been administered to laboratory workers who contact the pathogen on a regular basis.

Vaccines against several diseases that are of concern as biological weapons have not yet been developed. Plague is caused by a bacterium *Yersinia pestis* that is often carried by rat mites. Although research is ongoing, there is no vaccine against this disease and one is unlikely to be developed for several years. Botulism is caused by a toxin produced by the bacterium *Clostridium botulinum*. Although an antitoxin that reduces the severity of the symptoms is available, there is no vaccine against botulism. Viral hemorrhagic fevers are caused by any one of several viruses including Ebola, Marburg, Lassa and Machupo. No vaccine against these pathogens is currently available.

#### ■ FURTHER READING:

##### BOOKS:

- Joellenbeck, L. M., L. L. Zwanziger, J. S. Durch, et al. *The Anthrax Vaccine: Is It Safe? Does It Work?* Washington, DC: National Academies Press, 2002.
- Preston, R. *The Demon in the Freezer*. New York: Random House, 2002.

##### PERIODICALS:

- Bradley, K. A., J. Mogridge, M. Mourey, et al. "Identification of the Cellular Receptor for Anthrax Toxin." *Nature* no. 414 (2001): 225–29.
- Friedlander, A. M. "Tackling Anthrax." *Nature* no. 414 (2001): 160–61.
- Henderson, D. A. "Smallpox: Clinical and Epidemiologic Features." *Emerging Infectious Diseases* no. 5 (1999): 537–39.

Rosenthal, S. R., M. Merchlinsky, C. Kleppinger, et al. "Developing New Smallpox Vaccines." *Emerging Infectious Diseases* no. 7 (2001): 920–26.

##### ELECTRONIC:

- Centers for Disease Control and Prevention. "Smallpox Factsheet: Vaccine Overview." Public Health Emergency Preparedness and Response. December 9, 2002. <<http://www.bt.cdc.gov/agent/smallpox/vaccination/facts.asp>>(31 December 2002).
- Rhode Island Department of Health: Bioterrorism Preparedness Program "History of Biological Warfare and Current Threat." <<http://www.healthri.org/environment/biot/history.htm>> (March 12, 2003).

##### SEE ALSO

*Anthrax Vaccine*  
*Biomedical Technologies*  
*Biological Warfare*  
*Pathogen Transmission*  
*Surgeon General and Nuclear, Biological, and Chemical Defense, United States Office*  
*Variola Virus*

## Variola Virus

■ JULI BERWALD

Variola virus (or *variola major*) is the virus that causes smallpox. The virus is one of the members of the poxvirus group (*Poxviridae*) and it is one of the most complicated animal viruses. The variola virus is extremely virulent and is among the most dangerous of all the potential biological weapons.

The variola virus particle is shaped like a biconcave brick 200 to 400 nm long. Its inner compartment contains a highly compressed double strand of deoxyribonucleic acid as well as about 100 proteins and 10 viral enzymes. The enzymes are used in nucleic acid replication. Variola DNA contains about 250,000 base pairs, which make up about 200 genes. The depressions in the brick shape contain structures called lateral bodies, whose function is unknown. Two layers of membrane surround the outside of the virus. The outer layer is covered with spikes 20 nm long that are sometimes arranged helically.

The variola virus attaches to membrane receptors on the exterior of the host cell. The exact mechanisms involved in the binding to and penetration of the host membrane are not known. As it enters the cell, however, the virus loses its exterior membrane coat. Once inside the cell the interior membrane layer is removed and the virus's proteins, enzymes and DNA are released into the cytoplasm of the host cell where viral replication and assembly takes place. The first step in replicating the virus DNA involves a particular set of virus enzymes called Type

I topoisomerase enzymes, which uncoil the compressed strands of variola DNA and aid in replicated the *early genes*. The second step of genome replication involves replicating the *late genes*. During the replication of the variola DNA, large concatamers are formed and subsequently cleaved to form individual virus genomes. The variola virus appears to be able to replicate itself without using any of the host cell's replication machinery. Individual viruses are assembled with the help of the Type I topoisomerase enzymes. It is thought that viral membranes are taken from the cisternae between the host's Golgi apparatus and endoplasmic reticulum. As new viruses are released from the host cell, this Golgi derived membrane is traded for the host's cell membrane. Release occurs about 12 hours after initial infection. The production of variola virus by the host cell usually results in host cell death.

Variola virus infects only humans and can be easily transmitted from person to person via the air. Inhalation of only a few virus particles is sufficient to establish an infection. Transmission of the virus is also possible if items such as contaminated linen are handled. The common symptoms of smallpox include chills, high fever, extreme tiredness, headache, backache, vomiting, sore throat with a cough, and sores on mucus membranes and on the skin. As the sores burst and release pus, the afflicted person can experience great pain. Males and females of all ages are equally susceptible to infection. Prior to smallpox eradication approximately one third of patients died—usually within a period of two to three weeks following appearance of symptoms.

The origin of the variola virus is not clear. However, the similarity of the virus and cowpox virus has prompted the suggestion that the variola virus is a mutated version of the cowpox virus. The mutation likely allowed the virus to infect humans. If such a mutation did occur, then it is possible that when early humans became more agricultural and less nomadic, there may have been selective pressure for the cowpox virus to adapt the capability to infect humans.

Vaccination to prevent infection by the variola virus was established in the 1700s. English socialite and public health advocate Lady Mary Wortley Montagu popularized the practice of injection with the pus obtained from smallpox sores as a protection against the disease. This technique became known as variolation. Late in the same century, Edward Jenner successfully prevented the occurrence of smallpox by an injection of pus from cowpox sores. This was the first vaccination. Vaccination against smallpox has been very successful, and the variola virus is the only pathogenic virus that has been eliminated from the natural environment. The last recorded case of smallpox infection was in 1977. Routine vaccination against smallpox was discontinued in the 1980s.

In the late 1990s, a resolution was passed at the World Health Assembly directing that the remaining stocks of variola virus be destroyed to prevent the reemergence of

smallpox and the misuse of the variola virus as a biological weapon. At the time only two high-security laboratories were thought to contain variola virus stock: the Centers for Disease Control and Prevention in Atlanta, Georgia, and the Russian State Center for Research on Virology and Biotechnology in Koltsovo, Russia. However, this decision was postponed until 2002, and now the United States government has indicated its unwillingness to comply with the resolution because of security issues related to potential bioterrorism. Destruction of the stocks of variola virus would deprive countries of the material needed to prepare vaccine in the event of the deliberate use of the virus as a biological weapon. This scenario has gained more credence in the past decade, as terrorist groups have demonstrated the resolve to use biological weapons, including smallpox. In addition, intelligence agencies in several Western European countries issued opinions that additional stocks of the variola virus exist in other than the previously authorized locations.

#### ■ FURTHER READING:

##### BOOKS:

- Hopkins, D. R. *The Greatest Killer: Smallpox in History*. Chicago: University of Chicago Press, 2002.
- Preston, R. *The Demon in the Freezer*. New York: Random House, 2002.

##### PERIODICALS:

- Henderson, D. A., T. V. Inglesby, and J. G. Bartlett, et al. "Smallpox as a Biological Weapon: Medical and Public Health Management." *Journal of the American Medical Association* no. 281 (1999): 2127–37.

##### ELECTRONIC:

- Centers for Disease Control and Prevention. "Smallpox." Public Health Emergency Preparedness and Response. November 26, 2002. <<http://www.bt.cdc.gov/agent/smallpox/index.asp>>(27 November 2002).

##### SEE ALSO

- Biocontainment Laboratories*  
*Biological and Toxin Weapons Convention*  
*Biological Warfare*  
*Biological Warfare, Advanced Diagnostics*  
*Biological Weapons, Genetic Identification*  
*CDC (United States Centers for Disease Control and Prevention)*

---

## Venezuela, Intelligence and Security

---

Since civilian government was restored in 1958, the Venezuelan military and intelligence organizations have

generally operated under the control of a representative democratic government and a succession of democratically elected presidents.

Prior to 1958 Venezuela was governed by a series of *caudillos* (military or military-controlled governments). Post–World War II transformations in the economy, spurred by the discovery of major oil reserves, resulted in both internal and external pressures to reform Venezuelan government.

Venezuela is a member of OPEC (Organization of Petroleum Exporting Countries), the world's fifth-largest oil producer, and is a major supplier of oil to the United States.

In 2000, social unrest again began to increase in Venezuela and general strikes shut down the oil industry. As of May 2003, confrontations between strikers and government forces have imperiled the continuation in office of chief of state President Hugo Chavez. The military has shown signs of impatience with Chavez's inability to restore order and start an economic recovery. Rumor of coup attempts started to surface in late 2002.

Venezuela continues to be a major exporter of cocaine to the U.S. and local drug-related battles along the border are frequent.

Venezuela's armed forces include the National Armed Forces (*Fuerzas Armadas Nacionales*), Naval Forces (*Fuerzas Navales*), Air Force (*Fuerzas Aereas*), Armed Forces of Cooperation or National Guard (*Fuerzas Armadas de Cooperacion* or *Guardia Nacional*).

Venezuela's intelligence agency is the Intelligence and Preventive Services Directorate (DISIP) but National Guard units have also cooperated with CIA operations.

Because of alleged involvement in the support of drug trafficking, sales of U.S. military hardware, including F-16s, in 1983 was highly controversial. At the time Venezuela was seen as one of the most stable Latin American countries and a U.S. ally against leftist intervention in Central and South America.

#### ■ FURTHER READING:

##### BOOKS:

Gilderhus, Mark T. *The Second Century: U.S.-Latin American Relations Since 1889*. Wilmington, DE: Scholarly Resources, 2000.

Hillman, Richard S., John A. Peeler, and Elsa Cardozo da Silva. *Democracy and Human Rights in Latin America*. Westport, CT: Praeger, 2002.

Musicant, Ivan. *The Banana Wars: A History of United States Military Intervention in Latin America from the Spanish-American War to the Invasion of Panama*. New York: Macmillan, 1990.

##### SEE ALSO

*Americas, Modern U.S. Security Policy and Interventions*

## Venona

■ ADRIENNE WILMOTH LERNER

The Venona Project was the United States Army's Signal Intelligence Service, and later the National Security Agency, operation to intercept and decrypt high-level Soviet diplomatic communications. The project formally began during World War II, though Soviet communications had been monitored occasionally since World War I. The long-running Venona Project spanned the length of the Cold War, ending in 1980 at the beginning of the period of détente preceding the fall of the Soviet Union. Venona decrypts lead to the arrest of several Soviet NKVD, later KGB, agents operating in the United States, and gave U.S. intelligence information regarding Soviet infiltration of sensitive government departments and classified projects.

**Key breakthroughs.** The U.S. Army's Signal Intelligence Service formally began the top-secret Venona Project on February 1, 1943. A team of cryptologists established project headquarters in the building of a former girls' school in Arlington, Virginia. The location became known as Arlington Hall. The Venona team began the difficult task of deciphering Soviet diplomatic intercepts gathered by U.S. intelligence since 1939. The collection was unsorted, unanalyzed, and in disarray, but the small Arlington Hall team quickly made key breakthroughs that allowed limited interpretation of the Soviet communications.

After sorting the intercepts by cipher system, origin, and recipient, cryptologists discovered that certain ciphers were used for certain missions. Diplomatic intercepts were different from Soviet intelligence communications, but many of the codes were variations of each other. In all, the initial team identified five separate cryptological systems.

Several key breakthroughs in the Venona Project facilitated the monitoring of Soviet communications by the U.S. intelligence community. Cryptographer Cecil Phillips observed mathematical patterns in one of the Soviet cryptosystems. While the full decoding of these messages remained illusive, the Arlington Hall team was able to identify intercepts from KGB communications. In October 1943, an archaeologist working as a wartime code breaker, Richard Hallock, discovered repetitions and patterns within other Soviet codes. This breakthrough led to the first partial decoding of Venona intercepts.

Over the next three years, the Arlington Hall team made substantial progress on cracking various Soviet codes. By 1943, most of the intercepts were double-ciphered, utilizing not only the Soviet codes, but also a mathematical encryption system. Without the fortune of recovering a lost Soviet codebook or cipher machine, Arlington Hall code breakers labored to break the complex code system by hand. By the end of World War II, intercepted Soviet communications were being decoded and

BRIDE

~~TOP SECRET~~

USSR

Ref. No: S/NBF/T284 (of 23/12/1952)

Issued: 5/4/1957

Copy No: 205

RE-ISSUE

THE SHADOWING OF "GNAT" (1945)

From: NEW YORK

To: MOSCOW

No: 87

19 Jan. 45

To VIKTOR[i].

[16 groups unrecovered]

ZENZINOV[ii]

[18 groups unrecovered]

DALLIN[iii] and allegedly KERENSKIJ[iv]

[21 groups unrecoverable]

the last three weeks GNAT [KOMAR][v] and DALLIN have been in a great panic. GNAT has noticed that he is being intensively shadowed; moreover he and D.[vi] have received warnings by telephone from some persons or other that CARTHAGE [KARFAGEN][vii] is preparing to hand GNAT over to the HOUSE [DQI][viii]. GNAT is alarmed by the incessant shadowing and is said to be hiring two bodyguards. D. says that he supposes that it is the "GPU"[ix] which is having GNAT shadowed, preparing to do away with him.

The work [OPORILENIE] on GNAT is being carried out by KANT[x] and JEMNE [ZHANNA][xi]. KANT is acquainted with GNAT personally, but [B% for the most part] gets his information through a neighbour[a].

Distribution

[Continued overleaf]

M.H. file  
KOMAR/GNAT

A decoded 1945 message suggesting worry about a soviet defector codenamed "Gnat" (Viktor Andreevich Kravchenko), one of thousands of secret KGB and GRU messages intercepted and decoded by the U.S. Signals Intelligence Unit, which was codenamed VENONA. NSA ARCHIVES.

read with some success, but the process of translating and analyzing the decrypted messages was painstakingly slow.

**Venona intelligence.** The first successful uses of intelligence information gathered by the Venona Project came in 1945. Though Venona intercepts could only be deciphered in part, and yielded scant information, two events verified their accuracy and uncompromised nature. As Cold War and anti-communist tensions rose in the United States, the FBI investigated the claims of several people who professed to have knowledge of Soviet espionage activities. Agents questioned Whittaker Chambers, who, as early as the 1930s, reported details of suspected Soviet espionage within the U.S. government. His claims had gone unnoticed in the previous decade, but Whittaker provided information on Soviet agents consistent with similar information in Venona intercepts. Later the same year, Elizabeth Bentley, a minor KGB agent and courier, provided FBI agents with a list of Soviet spies operating in the United States, and their codenames. Some of the codenames Bentley provided matched names that frequently appeared in Venona project messages. U.S. intelligence was thus assured that Soviet intelligence had no knowledge of the Venona Project, or the degree to which the security of Soviet diplomatic and intelligence communications had been compromised.

The following year, analyst Meredith Gardner decoded several portions of KGB messages, furthering decryption efforts begun on the cipher system by Cecil Phillips. The Venona team concentrated on decoding intelligence communications between Moscow and a KGB stronghold in New York City. Gardner decoded messages relayed two years earlier in 1944. In the wartime communications, Soviet officials discussed plans for foreign espionage, counterintelligence measures, and high-level secret American projects. Among the secrets passed between the New York KGB Residence and Moscow headquarters were communications regarding U.S. weapons development. Venona intercepts analyzed by Gardner revealed that Soviet intelligence gained top-secret information on the Manhattan Project, the United State's effort to develop the atomic bomb. Arlington Hall provided U.S. intelligence with evidence of an extensive Soviet espionage campaign within the United States. Venona intercepts also yielded information about Soviet intelligence efforts in Latin America and Western Europe.

As Venona intercepts yielded more information about Soviet infiltration of other Allied governments, United States officials shared the intelligence with Britain and France. In 1948, British cryptologists joined the Venona team. The Venona project monitored Soviet communications in the United States and Britain, ferreting out undercover Soviet intelligence agents in both governments. United States Venona intelligence was sent to the FBI and CIA, while MI-5 and MI-6 processed information from the British team.

**Breaking the Soviet espionage network in the United States.** Information from Venona intercepts led to the arrest of several Soviet spies in the United States. Since Venona documents were not analyzed as they were received, however, most of those identified foreign agents had given secrets to the Soviets during World War II. Though the Soviet Union was a military ally of the United States during the war, sharing secret information remained illegal. Immediately following the war, relations between the two countries deteriorated. Thus most of the Venona intercepts were translated and analyzed in the light of Cold War tensions.

Among the Soviet agents first identified by Venona communications were State Department officers Alger Hiss and Laurence Duggan who gave the Soviets wartime intelligence. Lauchlin Currie, a friend and aide to President Franklin D. Roosevelt, notified Soviet intelligence when agents operating in the United States were dubbed suspicious by U.S. intelligence and law enforcement. Duncan Lee, an assistant to OSS Chief William Donovan, divulged a plethora of intelligence secrets to Moscow. Three members of the Treasury Department sold the Soviets weapons designs, economic assessments, and other classified information. An NSA linguist, William Weisband, who briefly contributed to Venona by translating intercepts, notified Soviet intelligence of the project's existence.

After this early wave of arrests in the 1950s, several more agents were discovered and taken into custody in the following decades. However, the most notorious, and perhaps the most threatening to national security, of the agents identified by Venona intercepts was the network of Soviet atomic spies. Venona intercepts proved that Soviet agents had infiltrated most areas of the Manhattan Project, and had obtained secrets from ultra-secure sites such as the Oak Ridge and Los Alamos. In 1947, Gardner discovered that the Soviets had placed several intelligence sources in the War Department. While Gardner uncovered several dozen codenames in communications regarding atomic secrets, Venona intercepts added to the cases against spies Klaus Fuchs, Theodore Hall, and Julius Rosenberg.

The team first cracked Rosenberg's codenames, Liberal and Antenna, because of a carelessly coded intercept that used both of his cryptonym and also discussed his wife, Ethel, using her real name. The trial of Julius and Ethel Rosenberg drew a mixed public reaction. Federal prosecutors relied on other evidence, most of which was not as compelling, to convict most Soviet informants rather than expose Venona to the public. Historians and journalists who later investigated anomalies in the Rosenberg case similarly did not have access to Venona documents. Several cases, including that of the Rosenbergs, remained contentious within the general public until Venona documents began to be declassified in the mid-1990s.

Venona intercepts not only provided American and British intelligence with the identities of Soviet spies, they also provided information regarding Soviet intelligence

tradecraft. Through Venona communications, the U.S. intelligence community learned how the Soviet network functioned. Venona documents illustrate how agents were recruited. The messages detailed the use of dead letter drops and the process for arranging meetings between agents. Venona intercepts provided information on Soviet counterintelligence operations and efforts to locate defectors in the United States.

**The legacy of Venona.** During the course of the Venona Project, nearly 2,200 messages were intercepted, decoded, and translated. Though the project officially spanned decades, its greatest successes were in the first decade of the Cold War. The Arlington Hall team decoded most KGB messages intercepted between 1947 and 1952. Soviet diplomatic messages, which used a less complicated cipher and encryption system, were routinely broken until the Soviets changed the cipher in 1957. Messages were often reworked by intelligence personnel, especially when trying to crack recurring codenames.

While the Venona Project was largely a success for the United States, it did have limitations. Messages were difficult to decipher, and the project did not decode messages in real time. In the earliest years of the project, code breakers worked on intercepts that were two and three years old. The process was accelerated in 1953 when Venona code breakers received from U.S. military intelligence the remains of a partially charred Soviet codebook. The book aided cryptographers in breaking the overlaying encryption system of several codes.

The Venona project was so secretive that intelligence officials did not brief President Harry Truman on its existence for several years. Regardless of its secrecy in the United States, Soviet intelligence learned of the operation and conducted counterintelligence against the Venona Project. KGB defectors, agents who fled the Soviet Union for the United States and cooperated with U.S. officials, told U.S. intelligence that KGB headquarters had limited knowledge of the communications surveillance program. Soviet officials placed their confidence in their encryption systems and did not order an immediate change of codes to protect communications security. Soviet double agent and master spy Kim Philby visited Arlington Hall for briefings while stationed in Washington, D.C. between 1949 and 1951. Whether Philby provided KGB headquarters with a detailed report of Venona operations remains unknown, but again, the Soviets did not quickly change their cipher systems.

One of the most contentious assertions of Venona intelligence is the involvement of American political organizations, especially the American Communist Party, in Soviet-led espionage against U.S. interests. Venona intelligence was used to seek out Soviet agents of espionage, but some charge that the project conducted surveillance on citizens and contributed to McCarthy era anti-communist hysteria among government officials. Recently declassified Venona documents show real links between a

few radical socialist and communist organizations in the United States, and Soviet espionage during the 1940s through 1960s. However, the majority of American socialist and communist organizations were never mentioned in Venona messages and bore no connection to Soviet espionage efforts.

In 1995, the National Security Agency officially acknowledged the existence of the Venona Project and began the process of declassifying related documents. The declassified materials include project plans and specifications, case files, and copies of the decoded Soviet intercepts.

#### ■ FURTHER READING:

##### BOOKS:

Haynes, John E., and Harvey Klehr. *VENONA: Decoding Soviet Espionage in America*. New Haven, CT: Yale University Press, 1999.

##### PERIODICALS:

Hatch, David A. "VENONA: An Overview." *American Intelligence Journal* 17, no. 1/2 (1996): 71–77.

##### ELECTRONIC:

United States National Security Agency. *VENONA Project Declassified Documents*. <<http://www.nsa.gov/docs/Venona>> 2003.

##### SEE ALSO

*Cold War (1945–1950), The Start of the Atomic Age*  
*Cold War (1950–1972)*  
*Cold War (1972–1989): The Collapse of the Soviet Union*  
*Cryptonym*  
*KGB (Komitet Gosudarstvennoi Bezopasnosti, USSR Committee of State Security)*  
*NSA (United States National Security Agency)*

---

## Vietnam War

---

#### ■ JUDSON KNIGHT

The Vietnam War was a struggle between communist and pro-western forces that lasted from the end of World War II until 1975. The communist Viet Minh, or League for the Independence of Vietnam, sought to gain control of the entire nation from its stronghold in the north. Opposing it were, first, France, and later the United States and United Nations forces, who supported the non-communist forces in southern Vietnam. In 1975, in violation of a 1973 peace treaty negotiated to end United States military involvement in South Vietnam and active war against North Vietnam, North Vietnamese forces and South Vietnamese communist sympathizers seized control of South Vietnam





Converted T-28 trainer aircraft and 250-pound bombs used by Meo pilots of Vang Pao's "mini-Air Force," a CIA-sponsored unit that fought against the North Vietnamese in northern Laos in 1972. ©BETTMANN/CORBIS.

and reunited the two countries into a single communist country.

American involvement in Vietnam has long been a subject of controversy. The fighting depended, to a greater extent than in any conflict before, on the work of intelligence forces. Most notable among these were various U.S. military intelligence organizations, as well as the Central Intelligence Agency (CIA).

**Early stages.** Led by Ho Chi Minh (1890–1969), the Viet Minh aligned themselves with the Soviets from the 1920s. However, they configured their struggle not in traditional communist terms as a class struggle, but as a war for national independence and unity, and against foreign domination. Vietnam at the time was under French control as part of Indochina, and World War II provided the first opportunity for a Viet Minh uprising against the French, in 1940. France, by then aligned with the Axis under the Vichy government, rapidly suppressed the revolt. Nor did the free French, led by General Charles de Gaulle, welcome the idea of Vietnamese independence.

After the war was over, de Gaulle sent troops to resume control, and fighting broke out between French and Viet Minh forces on December 19, 1946. On May 7, 1954, the French garrison at Dien Bien Phu fell to the Viet

Minh after an eight-week siege. Two months later, in July 1954, the French signed the Geneva Accords, by which they formally withdrew from Vietnam.

The Geneva Accords divided the country along the 17th parallel, but this division was to be only temporary, pending elections in 1956. However, in 1955 Ngo Dinh Diem declared the southern portion of the nation the Republic of Vietnam, with a capital at Saigon. In 1956, Diem, with the backing of the United States, refused to allow elections, and fighting resumed. The conflict was now between South Vietnam and the communist republic of North Vietnam, whose capital was Hanoi. Fighting the Army of the Republic of Vietnam (ARVN) were not only the regular army forces of the North Vietnamese Army (NVA), but also Viet Cong, guerrillas from the South who had received training and arms from the North.

**American involvement.** President Dwight D. Eisenhower had already sent the first U.S. military and civilian advisers to Vietnam in 1955, and four years later, two military advisers became the first American casualties in the conflict. The administration of President John F. Kennedy greatly expanded U.S. commitments to Vietnam, such that by late 1962 the number of military advisers had grown to 11,000. At the same time, Washington's support for the unpopular



Former South Vietnamese commando Tran Quoc Hung, left, with fellow commando Pham Ngoc Khanh were recruited by the CIA as intelligence gatherers during the 1960s and 1970s. Both sought recognition for Vietnamese commandos who aided the CIA and the Department of Defense during the Vietnam conflict. AP/WIDE WORLD PHOTOS.

Diem had faded, and when American intelligence learned of plans for a coup by his generals, the United States did nothing to stop it. Diem was assassinated on November 1, 1963.

Under President Lyndon B. Johnson, U.S. participation in the Vietnam War reached its zenith. The beginnings of the full-scale commitment came after August 2, 1964, when North Vietnamese gunboats in the Gulf of Tonkin attacked the U.S. destroyer *Maddox*. Requesting power from Congress to strike back, Johnson received it in the form of the Gulf of Tonkin Resolution, which granted the president virtual *carte blanche* to prosecute the war in Vietnam.

**High point of the war.** As a result of his strengthened position to wage war, and still enjoying broad support from the American public, Johnson launched a bombing campaign against North Vietnam in late 1964, and again in

March 1965, after a Viet Cong attack on a U.S. installation at Pleiku. By June 1965, as the first U.S. ground troops arrived, U.S. troop strength stood at 50,000. By year's end, it would be near 200,000.

General William C. Westmoreland, who had assumed command of U.S. forces in Vietnam in June 1964, maintained that victory required a sufficient commitment of ground troops. Yet by the mid-1960s, the NVA had begun moving into the South via the Ho Chi Minh Trail, and as communist forces began to take more villages and hamlets, they seemed poised for victory. Johnson pledged greater support, but despite growing number of ground troops and intensive bombing of the North in 1967, U.S. victory remained elusive.

The turning point in the U.S. effort came on January 30, 1968, when the NVA and Viet Cong launched a surprise attack during celebrations of the Vietnamese lunar new year, or Tet. The Tet Offensive, though its value as a military victory for the North is questionable, was an

enormous psychological victory that convinced Americans that short of annihilation of North Vietnam—an unacceptable geopolitical alternative—they could not win a Korea-like standoff or outright victory in Vietnam. In March 1968, Johnson called for an end to bombing north of the 20th parallel, and announced that he would not seek reelection. Westmoreland, too, was relieved of duty.

**Withdrawal (1969–75).** The administration of President Richard Nixon in 1969 began withdrawing, and instituted a process of “Vietnamization,” or turning control of the war over to the South Vietnamese. In 1970, the most significant military activity took place in Cambodia and Laos, where U.S. B-52 bombers continually pounded the Ho Chi Minh Trail in an effort to cut off supply lines.

Despite the bombing campaign, undertaken in pursuit of Vietnamization and the goal of making the war winnable for the South, the North continued to advance. On January 27, 1973, the United States and North Vietnam signed the Paris Peace Accords, and U.S. military involvement in Vietnam ended.

During the two years that followed, the North Vietnamese gradually advanced on the South. On April 30, 1975, communist forces took control of Saigon as government members and supporters fled. On July 2, 1976, the country was formally united as the Socialist Republic of Vietnam, and Saigon renamed Ho Chi Minh City.

**The intelligence and special operations war.** Behind and alongside the military war was an intelligence and special operations war that likewise dated back to World War II. At that time, the United States, through the Organization of Strategic Services (OSS), actually worked closely with Viet Minh operatives, who OSS agents regarded as reliable allies against the Japanese. Friendly relations with the Americans continued after the Japanese surrender, when OSS supported the cause of Vietnamese independence.

This stance infuriated the French, who sought to reestablish control while avoiding common cause with the Viet Minh. They attempted to cultivate or create a number of local groups, among them a Vietnamese mafia-style organization, that would work on their behalf against the Viet Minh. These efforts, not to mention the participation of one of the world’s most well-trained special warfare contingents, the Foreign Legion, availed the French little gain.

**Special Forces, military intelligence, and CIA.** In the first major U.S. commitment to Vietnam, Kennedy brought to bear several powerful weapons that together signified his awareness that Vietnam was not a war like the others America had fought: the newly created Special Forces group, known popularly as the “Green Berets,” as well as CIA and a host of military intelligence organizations.

Though Special Forces are known popularly for their prowess in physical combat, their mission in Vietnam

from the beginning had a strong psychological warfare component. In May 1961, Kennedy committed 400 of these elite troops to the war in Southeast Asia, and more would follow.

Alongside them, in many cases, were military intelligence personnel, whose ranks in Vietnam numbered 3,000 by 1967. Most of these were in two army units, the Army Security Agency (ASA) and the Military Intelligence Corps. The work of military intelligence ranged from the signals intelligence of ASA, one of whose members became the first regular-army U.S. soldier to die in combat in 1961, to the electronic intelligence conducted by navy destroyers such as the ill-fated *Maddox*. In addition, military aircraft such as the SR-71 Blackbird and U-2 conducted extensive aerial reconnaissance.

As for CIA, by the time the war reached its height in the mid- to late 1960s, it had some 700 personnel in Vietnam. Many of these operated undercover groups that included the Office of the Special Assistant to the Ambassador (OSA, led by future CIA chief William Colby), which occupied a large portion of the U.S. Embassy in Saigon.

**Cooperation and conflict.** These three major arms of the intelligence and special operations war—Special Forces and other elite units, military intelligence, and CIA—often worked together. When Kennedy sent in the first contingent of Special Forces, they went to work alongside CIA, to whom the president in 1962 gave responsibility for paramilitary operations in Vietnam.

Unbeknownst to most Americans, CIA was also in charge of paramilitary operations in two countries where the United States was not officially engaged: Cambodia and Laos. Long before Nixon’s campaign to cut off the Ho Chi Minh Trail with strategic bombers, CIA operatives were training a clandestine army of tribesmen and mercenaries in Laos. Ordinary U.S. troops were not involved in this sideshow war in the interior of Southeast Asia: only Special Forces, who—in order to conceal their identity as American troops—bore neither U.S. markings nor U.S. weaponry.

CIA and army intelligence personnel worked on another notorious operation, Phoenix, an attempt to seek out and neutralize communist personnel in South Vietnam during the period from 1967 to 1971. CIA claimed to have killed, captured, or turned as many as 60,000 enemy agents and guerrillas in Phoenix, a project noted for the ruthlessness with which it was carried out. In this undertaking, CIA and the army had the nominal assistance of South Vietnamese intelligence, but due to an abiding U.S. mistrust of their putative allies, the Americans gave the Saigon little actual role in Phoenix.

**The military and CIA debacles.** In other situations, CIA and military groups did not so much intentionally collaborate as they found themselves thrown together, often at cross-purposes, or at least in ways that were not mutually

beneficial. While U.S. Navy destroyers in the Gulf of Tonkin were monitoring North Vietnamese electronic transmissions, CIA was busy striking at Viet Minh naval facilities with fast craft whose South Vietnamese (or otherwise non-American) crews made CIA involvement deniable. But North Vietnamese intelligence was as capable as its military, and they fired on the *Maddox* in direct response to this CIA operation.

The U.S. military became involved in another CIA debacle when, in 1968, army intelligence tried to resume a failed effort by CIA's Studies and Observation Group (SOG), another cover organization. From the early 1960s, SOG had been attempting to parachute South Vietnamese agents into North Vietnam, with the intention of using them as saboteurs and agents provocateur. The effort backfired, with most of the infiltrators dead, imprisoned, or used by the North Vietnamese as bait. CIA put a stop to the undertaking, but army intelligence tried to succeed where CIA had failed—only to lose several hundred more Vietnamese agents.

The U.S. Air Force had to take over another unsuccessful CIA operation, Black Shield, which involved a series of reconnaissance flights by A-12 Oxcart spy planes over North Vietnam in 1967 and 1968. Using the A-12, which could reach speeds of Mach 3.1 (2,300 m.p.h. or 3,700 k.p.h.), Black Shield gathered extensive information on Soviet-built surface-to-air missile (SAM) installations in the North. To obtain the best possible photographic intelligence, the Oxcarts had to fly relatively low and slow, and in the fall of 1967 North Vietnamese SAMs hit—but did not down—an A-71. In 1968, the U.S. Air Force, operating SR-71 Blackbirds, replaced CIA.

**Assessing CIA in Vietnam.** Despite the notorious nature of Phoenix or the CIA undertakings in Cambodia and Laos, as well as the occasions when CIA overplayed its hand or placed the military in the position of cleaning up one of its failed operations, CIA involvement in Vietnam was far from an unbroken record of failure. One success was Air America. The latter, a proprietary airline chartered in 1949, supplied the secret war in the interior, and also undertook a number of other operations in Vietnam and other countries in Asia. That Air America was only disbanded in 1981, long after the war ended, illustrates its effectiveness.

The popular image of CIA operatives in Vietnam as fiends blinded by hatred of communism—an image bolstered by Hollywood—is as lacking in historical accuracy as it is in depth of characterization. Like other Americans involved in Vietnam, members of CIA began with the belief that they could and would save a vulnerable nation from Soviet-style totalitarianism and provide its people with an opportunity to develop democratic institutions, establish prosperity, and find peace. Much more quickly than their counterparts in the military and political communities, however, members of the intelligence community came to recognize the fallacies on which their undertaking was based.

**Intelligence vs. the military and the politicians.** Whereas many political and military leaders adhered to standard interpretations about the North Vietnamese, such as the idea that they were puppets of Moscow whose power depended entirely on force, CIA operatives with closer contact to actual Vietnamese sources recognized the appeal of the Viet Minh nationalist message. And because CIA recognized the strength of the enemy, their estimate of America's ability to win the war—particularly as the troop buildup began in the mid-1960s—became less and less optimistic.

CIA appraisal of the situation tended to be far less sanguine than that of General Westmoreland and other military leaders, and certainly less so than that of President Johnson and other political leaders far removed from the conflict. In 1965, for instance, CIA and the Defense Intelligence Agency (DIA) produced a joint study in which they predicted that the bombing campaign would do little to soften North Vietnam. This was not a position favored by Washington, however, so it received little attention.

Whereas Washington favored an air campaign, General Westmoreland maintained that the war would be won by ground forces. Both government and military leaders agreed on one approach: the use of statistics as a benchmark of success or failure. In terms of the number of bombs dropped, cities hit, or Viet Cong and NVA killed, American forces seemed to be winning. Yet for every guerrilla killed, the enemy seemed to produce two or three more in his place, and every village bombed seemed only to increase enemy resistance.

**The lessons of Vietnam.** In the end, the United States effort in Vietnam was undone by the singularity of aims possessed by its enemies in the North; the instability and unreliability of its allies in the South, combined with American refusal to give the South Vietnamese a greater role in their own war; and a divergence of aims on the part of American leaders.

For example, the Tet Offensive, which resulted in so many Viet Cong deaths that the guerrilla force was essentially eliminated, and NVA regulars took the place of the Viet Cong, is remembered as a *victory* for the North. And it was a victory in psychological, if not military, terms. The surprise, fear, and disappointment elicited by the Tet Offensive—combined with a rise of political dissent within the United States—punctured America's will to wage the war, and marked the beginning of the end of American participation in Vietnam.

For some time, U.S. college campuses had seen small protests against the war, but in 1968 the number of these demonstrations grew dramatically, as did the ranks of participants. Nor were youth the only Americans now opposing the war in large numbers: increasingly, other sectors of society—including influential figures in the media, politics, the arts, and even the sciences—began to make their opposition known. In the final years of Vietnam, there was a secondary war being fought in the

United States—a war concerning America’s vision of itself and its role in the world.

By war’s end, Vietnam itself had largely been forgotten. Despite earlier promises of a liberal democratic government, the unified socialist republic fell prey to the exigencies typical of communist dictatorship: mass imprisonments and executions, forced redistribution of land, and the banning of political opposition. Forgotten, too, were Laos and even Cambodia, where the Khmer Rouge launched a campaign of genocide that killed an estimated two million people.

The Vietnamese invasion in 1979 probably saved thousands of Cambodian lives, but in the aftermath, Vietnam came to be regarded as a colonialist power. The nation once admired by the third world for standing up to America now became a pariah, supported only by Moscow—which had gained access to a valuable warm-water port at Cam Ranh Bay—and its allies in Eastern Europe.

During the remainder of the 1970s, America was in retreat, its attention turned away from the fate of countries that fell to communism or, in the case of Iran, to Islamic fundamentalist dictatorship. Americans focused their anger on those they regarded as having led them astray during the war years: politicians, the military, and CIA, which came under intense scrutiny during the 1975–76 Church committee hearings in the U.S. Senate. Only in the 1980s, under President Ronald Reagan, did the United States return to an activist stance globally.

#### ■ FURTHER READING:

##### BOOKS:

Allen, George W. *None So Blind: A Personal Account of the Intelligence Failure in Vietnam*. Chicago: Ivan R. Dee, 2001.

Conboy, Kenneth K., and Dale Andradé. *Spies and Commandos: How America Lost the Secret War in North Vietnam*. Lawrence, KS: University Press of Kansas, 2000.

Kissinger, Henry. *Years of Renewal*. New York: Simon and Schuster, 1999.

Shultz, Richard G. *The Secret War against Hanoi: Kennedy’s and Johnson’s Use of Spies, Saboteurs, and Covert Warriors in North Vietnam*. New York: HarperCollins, 1999.

Sorley, Lewis. *A Better War: The Unexamined Victories and Final Tragedy of America’s Last Years in Vietnam*. New York: Harcourt Brace, 1999.

Wirtz, James J. *The Tet Offensive: Intelligence Failure in War*. Ithaca, NY: Cornell University Press, 1991.

##### ELECTRONIC:

Vietnam War Declassification Project. Gerald R. Ford Library and Museum. <<http://www.ford.utexas.edu/library/exhibits/vietnam/>> (February 5, 2003).

##### SEE ALSO

CIA (*United States Central Intelligence Agency*)

*Cold War (1950–1972)*

*Cold War (1972–1989): The Collapse of the Soviet Union Johnson Administration (1963–1969), United States National Security Policy*

*Kennedy Administration (1961–1963), United States National Security Policy*

*Nixon Administration (1969–1974), United States National Security Policy*

## Viral Biology

■ BRIAN D. HOYLE/ABDEL HAKIM NASR

An understanding of the fundamentals of virus structure, genetics, and replication is critical to virologists and other forensic investigators attempting to identify potential biogenic pathogens that may be exploited as agents in biological warfare or by bioterrorists.

### Fundamentals of Viral Biology

Viruses are essentially nonliving repositories of nucleic acid that require the presence of a living prokaryotic or eukaryotic cell for the replication of the nucleic acid. There are a number of different viruses that challenge the human immune system and that may produce disease in humans. In general, a virus is a small, infectious agent that consists of a core of genetic material (either deoxyribonucleic acid [DNA] or ribonucleic acid [RNA]) surrounded by a shell of protein. All viruses share the need for a host in order to replicate their deoxyribonucleic acid (DNA) or ribonucleic acid (RNA). The virus commandeers the host’s existing molecules for the nucleic acid replication process. There are a number of different viruses. The differences include the disease symptoms they cause, their antigenic composition, type of nucleic acid residing in the virus particle, the way the nucleic acid is arranged, the shape of the virus, and the fate of the replicated DNA. These differences are used to classify the viruses and have often been the basis on which the various types of viruses were named.

**Virology, viral classification, types of viruses.** Virology is the discipline of microbiology that is concerned with the study of viruses. Viruses can exist in a variety of hosts. Viruses can infect animals (including humans), plants, fungi, birds, aquatic organisms, protozoa, bacteria, and insects. Some viruses are able to infect several of these hosts, while other viruses are exclusive to one host.

The classification of viruses operates by use of the same structure that governs the classification of bacteria. The International Committee on Taxonomy of Viruses established the viral classification scheme in 1966. From the broadest to the narrowest level of classification, the viral scheme is: Order, Family, Subfamily, Genus, Species,



A man leaves his house while it is fumigated for mosquitos in Costa Rica in an effort to stop a 2002 outbreak of Dengue fever, whose viral hemorrhagic variety can be fatal if not immediately treated. AP/WIDE WORLD PHOTOS.

and Strain/type. To use an example, the virus that was responsible for an outbreak of Ebola hemorrhagic fever in a region of Africa called Kikwit is classified as Order Mononegavirales, Family Filoviridae, Genus *Filovirus*, and Species Ebola virus Zaire.

In the viral classification scheme, all families end in the suffix *viridae*, for example Picornaviridae. Genera have the suffix *virus*. For example, in the family Picornaviridae there are five genera: enterovirus, cardiovirus, rhinovirus, aphthovirus, and hepatovirus. The names of the genera typically derive from the preferred location of the virus in the body (for those viral genera that infect humans). As examples, rhinovirus is localized in the nasal and throat passages, and hepatovirus is localized in the liver. Finally, within each genera there can be several species.

There are a number of criteria by which members of one grouping of viruses can be distinguished from those in another group. For the purposes of classification, however, three criteria are paramount. These criteria are the host organism or organisms that the virus utilizes, the shape of the virus particle, and the type and arrangement of the viral nucleic acid.

An important means of classifying viruses concerns the type and arrangement of nucleic acid in the virus

particle. Some viruses have two strands of DNA, analogous to the double helix of DNA that is present in prokaryotes such as bacteria and in eukaryotic cells. Some viruses, such as the Adenoviruses, replicate in the nucleus of the host using the replication machinery of the host. Other viruses, such as the Poxviruses, do not integrate in the host genome, but replicate in the cytoplasm of the host. Another example of a double-stranded DNA virus are the Herpesviruses.

Other viruses only have a single strand of DNA. An example is the Parvoviruses. Viruses such as the Parvoviruses replicate their DNA in the host's nucleus. The replication involves the formation of what is termed a negative-sense strand of DNA, which is a blueprint for the subsequent formation of the RNA and DNA used to manufacture the new virus particles.

The genome of other viruses, such as Reoviruses and Birnaviruses, is comprised of double-stranded RNA. Portions of the RNA function independently in the production of a number of so-called messenger RNAs, each of which produces a protein that is used in the production of new viruses.

Still other viruses contain a single strand of RNA. In some of the single-stranded RNA viruses, such as Picornaviruses, Togaviruses, and the Hepatitis A virus, the

RNA is read in a direction that is termed “+ sense.” The sense strand is used to make the protein products that form the new virus particles. Other single-stranded RNA viruses contain what is termed a negative-sense strand. Examples are the Orthomyxoviruses and the Rhabdoviruses. The negative strand is the blueprint for the formation of the messenger RNAs that are required for production of the various viral proteins.

Still another group of viruses have + sense RNA that is used to make a DNA intermediate. The intermediate is used to manufacture the RNA that is eventually packaged into the new virus particles. The main example is the Retroviruses (e.g. the Human Immunodeficiency viruses). Finally, a group of viruses consist of double-stranded DNA that is used to produce a RNA intermediate. An example is the Hepadnaviruses.

An aspect of virology is the identification of viruses. Often, the diagnosis of a viral illness relies, at least initially, on the visual detection of the virus. For this analysis, samples are prepared for electron microscopy using a technique called negative staining, which highlights surface detail of the virus particles. For this analysis, the shape of the virus is an important feature.

A particular virus will have a particular shape. For example, viruses that specifically infect bacteria, the so-called bacteriophages, look similar to the Apollo lunar lander (LEM spacecraft). A head region containing the nucleic acid is supported on a number of spider-like legs. Upon encountering a suitable bacterial surface, the virus acts like a syringe, to introduce the nucleic acid into the cytoplasm of the bacterium.

Other viruses have different shapes. These include spheres, ovals, worm-like forms, and even irregular (pleomorphic) arrangements. Some viruses, such as the influenza virus, have projections sticking out from the surface of the virus. These are crucial to the infectious process.

As new species of eukaryotic and prokaryotic organisms are discovered, no doubt the list of viral species will continue to grow.

**Viral genetics.** Viral genetics, the study of the genetic mechanisms that operate during the life cycle of viruses, utilizes biophysical, biological, and genetic analyses to study the viral genome and its variation.

The virus genome consists of only one type of nucleic acid, which could be a single or double stranded DNA or RNA. Single stranded RNA viruses could contain positive-sense (+RNA), which serves directly as mRNA or negative-sense RNA (–RNA) that must use an RNA polymerase to synthesize a complementary positive strand to serve as mRNA. Viruses are obligate parasites that are completely dependant on the host cell for the replication and transcription of their genomes as well as the translation of the

mRNA transcripts into proteins. Viral proteins usually have a structural function, making up a shell around the genome, but may contain some enzymes that are necessary for the virus replication and life cycle in the host cell. Both bacterial virus (bacteriophages) and animal viruses play an important role as tools in molecular and cellular biology research.

Viruses are classified in two families depending on whether they have RNA or DNA genomes and whether these genomes are double or single stranded. Further subdivision into types takes into account whether the genome consists of a single RNA molecule or many molecules as in the case of segmented viruses. Four types of bacteriophages are widely used in biochemical and genetic research. These are the T phages, the temperate phages typified by bacteriophage lambda, the small DNA phages like M13, and the RNA phages. Animal viruses are subdivided in many classes and types. Class I viruses contain a single molecule of double stranded DNA and are exemplified by adenovirus, simian virus 40 (SV40), herpes viruses and human papillomaviruses. Class II viruses are also called parvoviruses and are made of single stranded DNA that is copied in to double stranded DNA before transcription in the host cell. Class III viruses are double stranded RNA viruses that have segmented genomes which means that they contain 10–12 separate double stranded RNA molecules. The negative strands serve as template for mRNA synthesis. Class IV viruses, typified by poliovirus, have single plus strand genomic RNA that serves as the mRNA. Class V viruses contain a single negative strand RNA which serves as the template for the production of mRNA by specific virus enzymes. Class VI viruses are also known as retroviruses and contain double stranded RNA genome. These viruses have an enzyme called reverse transcriptase that can both copy minus strand DNA from genomic RNA catalyze the synthesis of a complementary plus DNA strand. The resulting double stranded DNA is integrated in the host chromosome and is transcribed by the host own machinery. The resulting transcripts are either used to synthesize proteins or produce new viral particles. These new viruses are released by budding, usually without killing the host cell. Both HIV and HTLV viruses belong to this class of viruses.

Virus genetics is studied by either investigating genome mutations or exchange of genetic material during the life cycle of the virus. The frequency and types of genetic variations in the virus are influenced by the nature of the viral genome and its structure. Especially important are the type of the nucleic acid that influence the potential for the viral genome to integrate in the host, and the segmentation that influence exchange of genetic information through assortment and recombination.

Mutations in the virus genome could either occur spontaneously or be induced by physical and chemical means. Spontaneous mutations that arise naturally as a result of viral replication are either due to a defect in the genome replication machinery or to the incorporation of

an analogous base instead of the normal one. Induced virus mutants are obtained by either using chemical mutants like nitrous oxide that acts directly on bases and modify them or by incorporating already modified bases in the virus genome by adding these bases as substrates during virus replication. Physical agents such as ultraviolet light and x rays can also be used in inducing mutations. Genotypically, the induced mutations are usually point mutations, deletions, and rarely insertions. The phenotype of the induced mutants is usually varied. Some mutants are conditional lethal mutants. These could differ from the wild type virus by being sensitive to high or low temperature. A low temperature mutant would for example grow at 31°C but not at 38°, while the wild type will grow at both temperatures. A mutant could also be obtained that grows better at elevated temperatures than the wild type virus. These mutants are called hot mutants and may be more dangerous for the host because fever, which usually slows the growth of wild type virus, is ineffective in controlling them. Other mutants that are usually generated are those that show drug resistance, enzyme deficiency or an altered pathogenicity or host range. Some of these mutants cause milder symptoms compared to the parental virulent virus and usually have potential in vaccine development as exemplified by some types of influenza vaccines.

Besides mutation, new genetic variants of viruses also arise through exchange of genetic material by recombination and reassortment. Classical recombination involves breaking of covalent bonds within the virus nucleic acid and exchange of some DNA segments followed by rejoining of the DNA break. This type of recombination is almost exclusively reserved to DNA viruses and retroviruses. RNA viruses that do not have a DNA phase rarely use this mechanism. Recombination usually enables a virus to pick up genetic material from similar viruses and even from unrelated viruses and the eukaryotic host cells. Exchange of genetic material with the host is especially common with retroviruses. Reassortment is a non-classical kind of recombination that occurs if two variants of a segmented virus infect the same cell. The resulting progeny virions may get some segments from one parent and some from the other. All known segmented virus that infect humans are RNA viruses. The process of reassortment is very efficient in the exchange of genetic material and is used in the generation of viral vaccines especially in the case of influenza live vaccines. The ability of viruses to exchange genetic information through recombination is the basis for virus-based vectors in recombinant DNA technology and hold great promises in the development of gene therapy. Viruses are attractive as vectors in gene therapy because they can be targeted to specific tissues in the organs that the virus usually infect and because viruses do not need special chemical reagents called transfectants that are used to target a plasmid vector to the genome of the host.

Genetic variants generated through mutations, recombination or reassortment could interact with each

other if they infected the same host cell and prevent the appearance of any phenotype. This phenomenon, where each mutant provide the missing function of the other while both are still genotypically mutant, is known as complementation. It is used as an efficient tool to determine if mutations are in a unique or in different genes and to reveal the minimum number of genes affecting a function. Temperature sensitive mutants that have the same mutation in the same gene will for example not be able to complement each other. It is important to distinguish complementation from multiplicity reactivation where a higher dose of inactivated mutants will be reactivated and infect a cell because these inactivated viruses cooperate in a poorly understood process. This reactivation probably involves both a complementation step that allows defective viruses to replicate and a recombination step resulting in new genotypes and sometimes regeneration of the wild type. The viruses that need complementation to achieve an infectious cycle are usually referred to as defective mutants and the complementing virus is the helper virus. In some cases, the defective virus may interfere with and reduce the infectivity of the helper virus by competing with it for some factors that are involved in the viral life cycle. These defective viruses called “defective interfering” are sometimes involved in modulating natural infections. Different wild type viruses that infect the same cell may exchange coat components without any exchange of genetic material. This phenomenon, known as phenotypic mixing is usually restricted to related viruses and may change both the morphology of the packaged virus and the tropism or tissue specificity of these infectious agents.

**Virus replication.** Viral replication refers to the means by which virus particles make new copies of themselves. Although precise mechanisms vary, viruses cause disease by infecting a host cell and commandeering the host cell's synthetic capabilities to produce more viruses. The newly made viruses then leave the host cell, sometimes killing it in the process, and proceed to infect other cells within the host.

Viruses cannot replicate by themselves. They require the participation of the replication equipment of the host cell that they infect in order to replicate. The molecular means by which this replication takes place varies, depending upon the type of virus.

Viral replication can be divided up into three phases: initiation, replication, and release.

The initiation phase occurs when the virus particle attaches to the surface of the host cell, penetrates into the cell and undergoes a process known as uncoating, where the viral genetic material is released from the virus into the host cell's cytoplasm. The attachment typically involves the recognition of some host surface molecules by a corresponding molecule on the surface of the virus. These two molecules can associate tightly with one another, binding the virus particle to the surface. A well-studied



example is the haemagglutinin receptor of the influenzae virus. The receptors of many other viruses have also been characterized.

A virus particle may have more than one receptor molecule, to permit the recognition of different host molecules, or of different regions of a single host molecule. The molecules on the host surface that are recognized tend to be those that are known as glycoproteins. For example, the human immunodeficiency virus recognizes a host glycoprotein called CD4. Cells lacking CD4 cannot, for example, bind the HIV particle.

Penetration of the bound virus into the host interior requires energy. Accordingly, penetration is an active step, not a passive process. The penetration process can occur by several means. For some viruses, the entire particle is engulfed by a membrane-enclosed bag produced by the host (a vesicle) and is drawn into the cell. This process is called endocytosis. Polio virus and orthomyxovirus enters a cell via this route. A second method of penetration involves the fusion of the viral membrane with the host membrane. Then the viral contents are directly released into the host. HIV, paramyxoviruses, and herpes viruses use this route. Finally, but more rarely, a virus particle can be transported across the host membrane. For example, poliovirus can cause the formation of a pore through the host membrane. The viral DNA is then released into the pore and passes across to the inside of the host cell.

Once inside the host, the viruses that have entered via endocytosis or transport across the host membrane need to release their genetic material. With poxvirus, viral proteins made after the entry of the virus into the host are needed for uncoating. Other viruses, such as adenoviruses, herpesviruses, and papovaviruses associate with the host membrane that surrounds the nucleus prior to uncoating. They are guided to the nuclear membrane by the presence of so-called nuclear localization signals, which are highly charged viral proteins. The viral genetic material then enters the nucleus via pores in the membrane. The precise molecular details of this process remains unclear for many viruses.

For animal viruses, the uncoating phase is also referred to as the eclipse phase. No infectious virus particles can be detected during that 10 to 12 hour period of time.

In the replication, or synthetic, phase the viral genetic material is converted to deoxyribonucleic acid (DNA), if the material originally present in the viral particle is ribonucleic acid (RNA). This so-called reverse transcription process needs to occur in retroviruses, such as HIV. The DNA is imported into the host nucleus where the production of new DNA, RNA, and protein can occur. The replication phase varies greatly from virus type to virus type. However, in general, proteins are manufactured to ensure that the cell's replication machinery is harnessed to permit replication of the viral genetic material, to ensure that this replication of the genetic material does indeed occur, and

to ensure that this newly made material is properly packaged into new virus particles.

Replication of the viral material can be a complicated process, with different stretches of the genetic material being transcribed simultaneously, with some of these gene products required for the transcription of other viral genes. Also replication can occur along a straight stretch of DNA, or when the DNA is circular (the so-called "rolling circle" form). RNA-containing viruses must also undergo a reverse transcription from DNA to RNA prior to packaging of the genetic material into the new virus particles.

In the final stage, the viral particles are assembled and exit the host cell. The assembly process can involve helper proteins, made by the virus or the host. These are also called chaperones. Other viruses, such as tobacco mosaic virus, do not need these helper chaperones, as the proteins that form the building blocks of the new particles spontaneously self-assemble. In most cases, the assembly of viruses is symmetrical; that is, the structure is the same throughout the viral particle. For example, in the tobacco mosaic virus, the proteins constituents associate with each other at a slight angle, producing a symmetrical helix. Addition of more particles causes the helix to coil "upward" forming a particle. An exception to the symmetrical assembly is the bacteriophage. These viruses have a head region that is supported by legs that are very different in structure. Bacteriophage assembly is very highly coordinated, involving the separate manufacture of the component parts and the direct fitting together of the components in a sequential fashion.

Release of viruses can occur by a process called budding. A membrane "bleb" containing the virus particle is formed at the surface of the cell and is pinched off. For herpes virus this is in fact how the viral membrane is acquired. In other words, the viral membrane is a host-derived membrane. Other viruses, such as bacteriophage, may burst the host cell, spewing out the many progeny virus particles. But many viruses do not adopt such a host destructive process, as it limits the time of an infection due to destruction of the host cells needed for future replication.

## ■ FURTHER READING:

### BOOKS:

- Doerfler, Walter, and Petra Bohm, eds. *Virus Strategies: Molecular Biology and Pathogenesis*. New York: VCH, 1993.
- Flint, S. J., et al. *Principles of Virology: Molecular Biology, Pathogenesis, and Control*. Washington: American Society for Microbiology, 1999.
- Kurstak, Edouard, ed. *Control of Virus Diseases*. New York: Marcel Dekker, 1993.
- Richman, D. D., and R. J. Whitley. *Clinical Virology*. 2nd ed. Washington: American Society for Microbiology, 2002.
- Thomas, D. Brian. *Viruses and the Cellular Immune Response*. New York: Marcel Dekker, 1993.

## PERIODICALS:

Peters, C. J., and J. W. LeDuc. "An Introduction to Ebola: The Virus and the Disease." *The Journal of Infectious Diseases* no. 179 (Supplement 1, February 1999): ix–xvi.

## ELECTRONIC:

Biology Pages. "Viruses." 2002. <<http://www.ultranet.com/~jkimball/BiologyPages/V/Viruses.htm>> (April 12, 2003).

## SEE ALSO

*Bacterial Biology*  
*Biological and Toxin Weapons Convention*  
*Biological Warfare*  
*Biological Weapons, Genetic Identification*  
*Bioshield Project*  
*Bioterrorism*  
*Bioterrorism, Protective Measures*

## Viral Exposure Therapy, Antiviral Drug Development

■ BRIAN D. HOYLE

Several National Institute of Health and Defense Department funded programs are currently attempting to develop drugs that can be used to combat viruses most likely to be used by bioterrorists.

Antiviral drugs are compounds that are used to prevent or treat viral infections via the disruption of an infectious mechanism used by the virus, or to treat the symptoms of an infection. In addition to the development of vaccines, researchers are attempting to develop fast action identification and pharmacogenetic protocols for the development of effective anti-viral drugs that could potentially remediate some of the symptoms of viral exposure or early stage infection.

Different types of antiviral drugs have different modes of operation. One specific class of antiviral drugs are known as the antiretroviral drugs. These drugs target those viruses of clinical significance called retroviruses that use the mechanism of reverse transcription to manufacture the genetic material needed for their replication. The prime example of a retrovirus is the Human immunodeficiency virus (HIV), which is the viral agent of acquired immunodeficiency syndrome (AIDS). The development of antiviral drugs has been stimulated by the efforts to combat HIV.

Specific antiviral agents are designed to thwart the replication of whatever virus they are directed against. One means to achieve this is by blocking the virus from commandeering the host cell's nuclear replication machinery in order to have its genetic material replicated

along with the host's genetic material. The virus is not killed directly. But the prevention of replication will prevent the numbers of viruses from increasing, giving the host's immune system time to deal with the stranded viruses.

The incorporation of the nucleotide building blocks into deoxyribonucleic acid (DNA) can be blocked using the drug idoxuridine or trifluridine. Both drugs replace the nucleoside thymidine, and its incorporation produces a nonfunctional DNA. However, the same thing happens to the host DNA. So, this antiviral drug is also an anti-host drug.

Blockage of the viral replicative pathway by mimicking nucleosides can also be successful. But, because the virus utilizes the host's genetic machinery, stopping the viral replication usually affects the host cell.

Another tack for antiviral drugs is to block a viral enzyme whose activity is crucial for replication of the viral genetic material. The drug is converted in the host cell to a compound that can out-compete another compound for the binding of the viral enzyme, DNA polymerase, which is responsible for building DNA. The incorporation of the drug into the viral DNA stops the formation of the DNA.

Other antiviral drugs are directed at the translation process, whereby the information from the viral genome that has been made into a template is read to produce the protein product. For example, the drug ribavirin—used to combat the 2003 global Severe Acute Respiratory Syndrome (SARS) pandemic—inhibits the formation of messenger ribonucleic acid.

Still other antiviral drugs are directed at earlier steps in the viral replication pathway (e.g., blocking penetration into the host cell or release of nuclear material).

Antiviral therapy also includes molecular approaches. The best example is the use of oligonucleotides. These are sequences of nucleotides that are specifically synthesized to be complementary with a target sequence of viral ribonucleic acid. By binding to the viral RNA, the oligonucleotide blocks the RNA from being used as a template to manufacture protein.

The use of antiviral drugs is not without risk. Host cell damage and other adverse host reactions can occur. Thus, the use of antiviral drugs is routinely accompanied by close clinical observation.

### ■ FURTHER READING:

## BOOKS:

Kurstak, Edouard, ed. *Control of Virus Diseases*. New York: Marcel Dekker, 1993.

## ELECTRONIC:

Pan American Health Organization, World Health Organization. *Severe Acute Respiratory Syndrome (SARS)*

<<http://www.paho.org/English/HCP/HCT/EER/sars.htm>> (April 6, 2003).

#### SEE ALSO

*Bioshield Project*  
*Bioterrorism, Protective Measures*  
*Viral Biology*

## Voice Alteration, Electronic

In most cases, voice alteration technologies are employed to obscure an individual's identity. The ability of to alter the voice, however, also can be very useful in intelligence gathering and espionage. Impersonating a target individual (e.g., a worker important in the hierarchy of an organization) can provide access to information that is privy to only a select group of people. As well, if the voice alteration is sufficiently close to the original, access to files or physical locations that are barred by voice recognition software can be granted.

Crude voice alteration can be achieved by physical training. Actors and singers, for example, can train their voices so that the speech or song "projects" to all areas of the theatre. Also, accents can be learned and mimicked with reasonable accuracy.

In this natural process the vocal cords function as the source of the sounds and the vocal tract functions as the filter that can alter the frequency and cadence of the speech. The results is the rising and falling tones and intensity of spoken words.

However, the use of electronic technology can achieve accurate vocal alterations that are not otherwise possible. For example, vocal cords can be trained to be able to adopt different pitches—that is, to be capable of vibrating at different frequencies, so as to produce sounds that have different tones. However, electronic alterations of pitch can widen the vocal deceptions that are possible. For example, a man's voice can be altered to sound absolutely convincingly like a woman's.

The alteration of pitch can also be deliberately done electronically by detecting the frequency pattern of the speaker, and of the particular phrase being spoken. On a screen, the pattern appears as a series of waves and troughs. The arrangement of the waves and troughs is characteristic to the word being spoken. For example, the word "cat" will produce a different pattern than the word "invisible." By applying an electronic filter (or "window"—actually one or more mathematical equations, or algorithms) to the frequency pattern, waves and troughs can be selectively eliminated or shifted up and down to produce a different frequency. An experienced technician or

sophisticated software program can alter a word so as to change the sound of the word (i.e., a higher or lower tone) without distorting the sound of the word. Thus, the altered speech is still recognizable and interpretable, but can sound like it is being spoken by another person.

Electronic voice alteration can be subtle or extreme. The latter is associated with the almost incomprehensible voices of anonymous witnesses. This type of voice alteration is actually a voice disguise. The intention is not to mimic a voice, but to scramble the voice patterns to make the identify of the speaker impossible to identify.

There are several different electronic means of voice alteration. One type is known as speech inversion. Here, the frequency signal is in effect turned inside out around a designated frequency. Put another way, the parts of the speech that are "high" are made to sound "low", and visa versa.

A voice can also be electronically jumbled, so that it sounds like gibberish. But codes assigned to sections of the speech allows the listener (who has the electronic codes) to put the words back in their proper order.

Another means of electronic voice alteration is known as speech encryption. Here, speech is digitized and the digital signal manipulated to make the text of the speech unrecognizable to the listener's ear. But, the speech can be decoded, or decrypted, at the receiving end to yield the original recognizable speech.

Hardware and software voice encryption systems are available. Machines connected to a telephone can alter a person's speech during the telephone conversation. Anyone eavesdropping on the conversation would be incapable of understanding what was being said. However, a legitimate listener, having a machine on his or her phone, would be capable of decrypting the conversation.

The United States government and military uses a telephone conversation scrambling software program and hardware called STU III (Secure Telephone Unit, Generation III).

Scrambling digital electronic information in relation to time can also accomplish voice alteration. An example includes the delay of information. While an effective means of altering a voice, the method can produce an echo, and so is unpleasantly distracting to listen to.

#### ■ FURTHER READING:

##### BOOKS:

Hollien, Harry Francis. *The Acoustics of Crime: The New Science of Forensic Acoustics*. New York: Plenum Press, 1990.

———. *Forensic Voice Identification*. New York: Academic Press, 2001.

##### SEE ALSO

*Cryptology, History*

*Electro-optical Intelligence  
Parabolic Microphones*

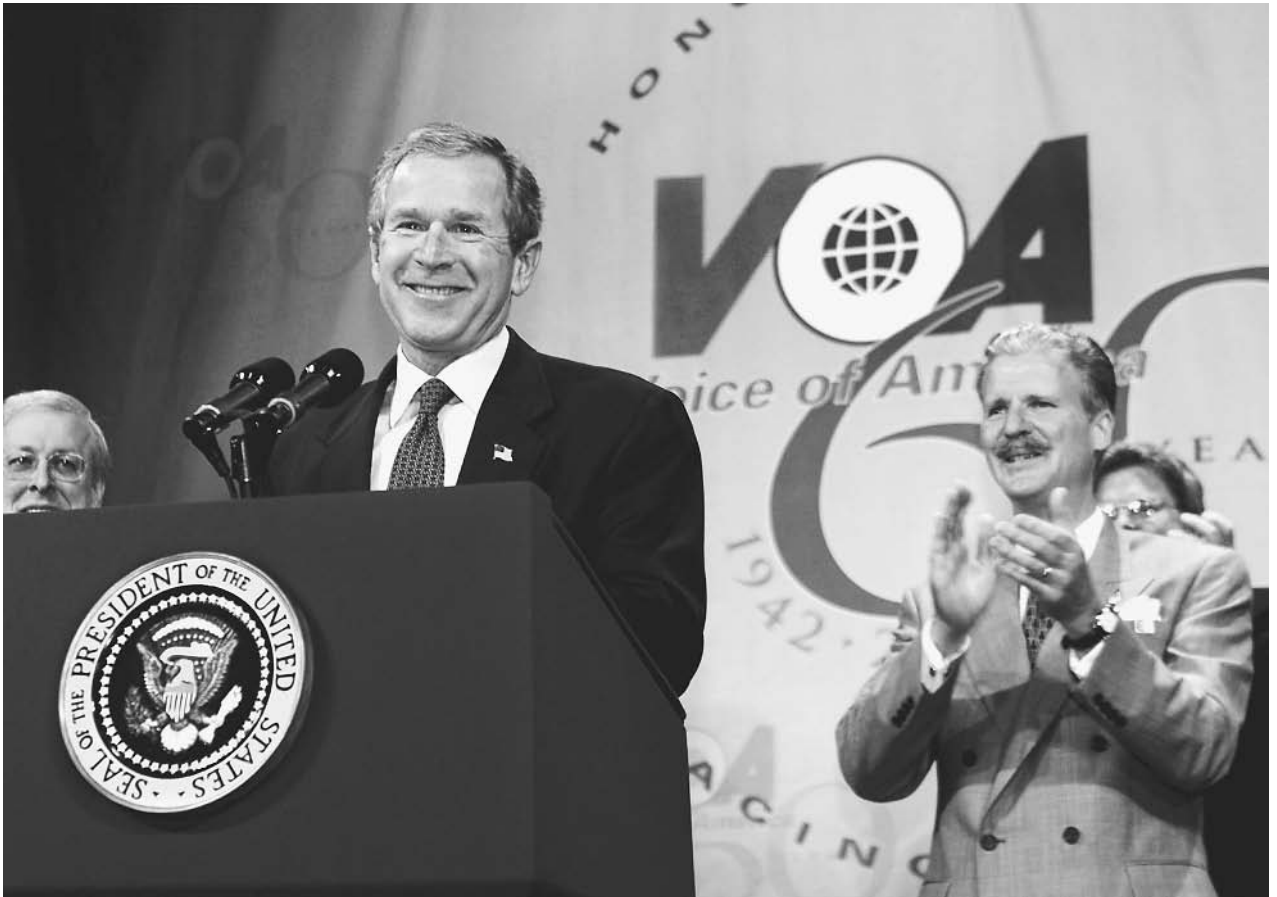
## Voice of America (VOA), United States

■ CARYN E. NEUMANN

The Voice of America (VOA) is a radio, television, and Internet news service that serves as the non-military voice of the United States government by communicating a comprehensive account of America and the world directly to people in other nations. Prohibited by law from broadcasting into the U.S., VOA uses 53 languages while transmitting more than 1,000 hours of news, informational, educational, and cultural programming every week from its Washington, D.C. headquarters to a worldwide audience of about 94 million people. Although the aim of VOA

is to promote the long-range interests of Americans, the news service is separated from the U.S. government by a firewall. It does not officially speak for the U.S. government, accepts no special treatment or assistance from American officials or government organizations, and strives for balanced and accurate news reporting. Separate sister agencies of VOA include Radio Free Europe, Radio Free Asia, and the Cuba-focused Radio Martí, with all of these information services overseen and guided by the Broadcasting Board of Governors.

VOA has evolved since its 1942 creation from an agitprop instrument that demanded action from its listeners to a news organization that calmly presents a balanced portrait of current events. In the 1930s, every major world power, especially that of Germany, capitalized on radio's potential to influence public opinion. The U.S., at that time less interested in playing a role in world affairs, did not see the value in developing a system of international radio propaganda. The fall of France, created in part by Nazi Germany's use of propaganda to destroy the French will to fight, changed U.S. opinion. President Franklin D. Roosevelt realized that ideas could be as useful as tanks in a military effort and he began to mobilize for propaganda



President Bush marks the 60th anniversary of Voice of America, a service that relays news to the world in 53 languages by radio, TV, and the Internet, at a celebration at VOA headquarters in Washington, D.C., in February 2002. AP/WIDE WORLD PHOTOS.

warfare. In 1941, Roosevelt established the U.S. Foreign Information Service (FIS) and the first U.S. government-sponsored radio broadcast was delivered on February 24, 1942 from New York City to Europe. In June 1942, the government established the Overseas Branch of the Office of War Information and six months later Roosevelt authorized the operation of VOA. The first VOA director, John Houseman, was an actor and playwright who used his dramatic skills to create agitprop. Under Houseman, every tone emanating from a VOA broadcast urged the French to join the resistance against the Nazis. Following the November 1942 Allied invasion of North Africa, VOA shifted its delivery style to calm and neutral news reporting that focused on the impending Allied liberation of Europe rather than the need for resistance.

The VOA seemed to be unnecessary once World War II had ended, but the start of the Cold War combined with hostile international broadcasting by the Soviet Union to make the news service into a valuable tool of democratic views. On August 1, 1953, VOA moved from its post-war location within the Department of State to join the newly formed U.S. Information Agency. The number of broadcasts delivered by VOA rose dramatically as the agency responded to the information needs of people behind the Iron Curtain and in politically unstable countries. In 1959, VOA inaugurated Special English, a slow-paced broadcast of simplified English for non-native speakers that was designed to facilitate comprehension. In 1994, VOA entered the television market with a Chinese-language program beamed by satellite. In 1996, VOA television studios were completed and the agency now simulcasts some portions of its programming on both radio and television in twelve languages: Albanian, Arabic, Bosnian, English, Indonesian, Mandarin Chinese, Persian, Russian, Serbian, Spanish, and Ukrainian. It also provides programming to 1200 radio stations around the world.

VOA's ability to broadcast consistently reliable and authoritative news to people in closed and war-torn societies makes it a valuable component of American security and intelligence efforts. Although it has occasionally come under attack by political leaders for failing to promote the overthrow of undemocratic governments, critics contend that VOA has succeeded in its mission of delivering unbiased news to a wide audience.

#### ■ FURTHER READING:

##### BOOKS:

- Fitzgerald, Merni Ingrassia. *The Voice of America*. New York: Dodd, Mead, 1987.
- Piresein, Robert William. *The Voice of America: A History of the International Broadcasting Activities of the United States Government 1940–1962*. New York: Arno Press, 1979.
- Shulman, Holly Cowan. *The Voice of America: Propaganda and Democracy 1941–1945*. Madison: The University of Wisconsin Press, 1990.

##### ELECTRONIC:

Voice of America. "About VOA." February 1, 2003. <<http://www.voa.gov/index.cfm>> (February 1, 2003).

##### SEE ALSO

*Cold War (1950–1972)*  
*Department of State, United States*  
*Information Warfare*

---

## Dozrozhdeniye Island, Soviet and Russian Biochemical Facility

---

■ BRIAN HOYLE

Vozrozhdeniye Island is a Russian island located in the Aral Sea approximately 1,300 miles to the east of Moscow that was used as a bioweapons test facility for the former Soviet Union. Since being decommissioned in the early 1990s the island has been left virtually unpatrolled. The island has served for decades as the repository of a large quantity of spores of *Bacillus anthracis*, the bacterial agent of anthrax, and other disease-causing bacteria and viruses. As the surrounding water has receded over the decades, direct access from the mainland to the island, and to the stocks of bioweapons that were disposed of by being buried on the island, will soon be possible. Concern is growing in the international community that the island will become a source of a new generation of bioweapons.

During its operation, the bioweapons facility on Vozrozhdeniye Island was regarded as an important strategy of the former Soviet Union in the tensions between the East and the West during the Cold War of the 1950s. Indeed, the word Vozrozhdeniye translates in Russian as "renaissance."

The island was used for open-air testing of bioweapons. The island was selected for its remote location and harsh conditions. The sparse vegetation and summer temperatures that reached 140 degrees Fahrenheit created inhospitable conditions that lessened the chances of survival for microorganisms that escaped. Records obtained following the island's decommissioning confirm that anthrax weapons were tested. As well, other microorganisms that were tested for their potential in biological warfare include the microbial agents of tularemia, plague, typhoid, and possibly smallpox.

The anthrax buried on the island was designed especially for the lethal use on humans in the time of war. The powder is a freeze-dried form of *Bacillus anthracis* called a

spore. A spore is a form of the some species of *Bacillus* and *Clostridium* that protects the organism's genetic material during times when conditions are not favorable for the survival of the actively growing form of the bacterium. Bacterial spores that are capable of resuscitation and growth have been recovered from samples over 100 years old. Resuscitation of the spore requires only suspension in growth media having the appropriate nutrients and incubation of the suspension at a temperature that is hospitable for the bacterial growth.

Following the banning of offensive biological weapons programs in the United States and Russia, the biological warfare agents on Vozrozhdeniye Island were buried on the island in 1988. The island was abandoned in 1991.

Vozrozhdeniye island has remained unguarded since 1991. Then, it was thought that the island's location in the middle of the large and geographically isolated Aral Sea made the island secure from entry. However, in the intervening decades the demands for irrigation water have caused the Aral Sea—the largest freshwater lake in the world—to be used as a source of irrigation water. Water has consistently been withdrawn faster than it can be replenished. As a result, the water level of the Aral Sea has declined drastically, so much so that many scientists now fear that Vozrozhdeniye Island might soon be directly connected to the mainland. If so, and if the island remains unguarded, the buried stockpiled weapons could be vulnerable to theft.

Additionally, some surveys of the island have indicated that migration of some of the buried material towards the surface is occurring. Upon surface exposure, the bacteria and viruses, which may still be capable of infection, could be spread in the wind or transported elsewhere by birds.

## ■ FURTHER READING:

### PERIODICALS:

Choffnes, E. "Germs on the Loose." *Bulletin of the Atomic Scientists* no. 57 (2001): 57–61.

### ELECTRONIC:

Monterey Institute of International Studies. "Former Soviet Biological Weapons Facilities in Kazakhstan: Past, Present, and Future." CNS Occasional Papers. 2002. <<http://cns.miis.edu/pubs/opapers/opl/opl.htm#island>>(28 December 2002).

National Aeronautics and Space Administration. "Rebirth Island Joins the Mainland." Earth Observatory. <[http://earthobservatory.nasa.gov/Newsroom/NewImages/images.php3?img\\_id=5108](http://earthobservatory.nasa.gov/Newsroom/NewImages/images.php3?img_id=5108)>(27 December 2002).

### SEE ALSO

*Biocontainment Laboratories*  
*Bioterrorism, Protective Measures*  
*Russia, Intelligence and Security*

## Vulnerability Assessments

As its name suggests, a vulnerability assessment is a test of a system to locate, diagnose, and correct areas of weakness that might make it susceptible in times of crisis, attack, or destabilization. Any system that is created, operated, and shaped by humans may qualify for, and may in fact require, a vulnerability assessment. The expression entered the English language in the 1980s and 1990s, and usage increased markedly after the terrorist attacks of September 2001. Vulnerability assessments have been applied to everything from computer networks to water systems.

In 1998 and 1999, Sandia National Laboratories in Albuquerque, New Mexico, in partnership with the National Law Enforcement and Corrections Technology Center-Southeast Region, assessed the vulnerability of several correctional facilities. The first step in such an assessment was to determine areas of vulnerability, and then to examine scenarios whereby those vulnerabilities are exploited. In the case of the prisons, the partnership examined classes of adversaries, including inmates and their families, along with tactics they might use, as well as all reasonable escape scenarios. It was noted that, rather than using a checklist in the design of prison security, it was advisable to apply a more advanced computer-driven analysis system. This would make it possible to consider all available means by which adversaries might achieve their objectives.

In June 2002, the nation's 54,000 drinking water systems and 16,000 wastewater agencies spent a combined \$700 million on vulnerability assessments, many of which had been spurred by the terrorist attacks of the preceding fall. At the same time, the Environmental Protection Agency (EPA) and the newly created Office (now Department) of Homeland Security had called for vulnerability assessments of critical infrastructure nationwide. Some industries welcomed this call as an opportunity for new business, but members of the oil and gas industry lobbied against a plan whereby companies would conduct vulnerability assessments and the EPA would assess compliance in certain areas. Meanwhile, vulnerability assessments have remained a powerful topic in the world of computers and cybersecurity. In January 2003, for instance, the Chemical Industry Date Exchange announced the formation of a new cybersecurity unit that would conduct a vulnerability assessment of chemical companies.

## ■ FURTHER READING:

### PERIODICALS:

"EPA Security Plan for Refining, Chemical Plants Blasted." *Oil & Gas Journal* 100, no. 39 (September 23, 2002): 22–24.

Giodano, Vincent. "Is It Right for Your Company?" *Communications News* 37, no. 9 (September 2000): 66–68.

- Landers, Jay. "Safeguarding Water Utilities." *Civil Engineering* 72, no. 6 (June 2002): 48–53.
- Seewald, Nancy. "CIDX Forms Cybersecurity Unit." *Chemical Week* 165, no. 2 (January 15, 2003): 20.
- Spencer, Debra D. "Vulnerability Assessment." *Corrections Today* 60, no. 4 (July 1998): 88–92.
- Wright, Andrew J., et. al. "War, Recession, and Growth." *ENR* 249, no. 2 (July 8, 2002): 34–36.

## SEE ALSO

*Critical Infrastructure  
Terrorism, Intelligence Based Threat and Risk Assessments*

## VX Agent

■ JULI BERWALD

VX nerve agent (O-ethyl S-[2-diisopropylaminoethyl] methylphosphonothioate) is one of the most toxic substances ever developed. Like other nerve agents, it is an organophosphate. Although it is often called a nerve gas, VX is usually a clear, odorless, tasteless liquid. A tiny amount of VX, about 10 mg—absorbed through the skin or eyes is fatal—and death usually occurs within an hour of exposure. VX poisons by binding to the enzyme cholinesterase and inactivating it. As a result, the chemical signals passed between nerve cells are transmitted uncontrollably. Symptoms of VX poisoning include constriction of the pupils, headache, runny nose, nasal congestion, chest tightness, giddiness, anxiety, and nausea, eventually progressing to convulsions and respiratory failure. VX poisoning can be treated immediately with two antidotes: atropine and pralidoxime chloride. Because of its extreme toxicity, VX is considered a weapon of mass destruction.

**VX poisoning.** Chemical signals are transmitted between nerve cells by means of small molecules called neurotransmitters. One of the most common neurotransmitters in the central and peripheral nervous system is acetylcholine. Under normal conditions, acetylcholine is released from the terminal axon of one nerve cell, crosses the synaptic cleft between nerve cells and binds with a receptor on the membrane of the post-synaptic nerve cell. Then, the enzyme cholinesterase binds to acetylcholine and inactivates it. This completes the chemical signaling between nerve cells.

When the VX nerve agent is present in the nervous system, it inactivates the enzyme cholinesterase. As a result, the receptor on the post-synaptic nerve cell is indefinitely stimulated by acetylcholine. In addition, the pre-synaptic nerve cell continues to release acetylcholine.

Nervous signals are never completed and the nervous system is eventually destroyed.

VX poisoning can occur by exposure to the eyes or skin, inhalation, or ingestion. Symptoms occur within minutes. Autonomic nervous system symptoms include constricted pupils, reduced vision and other visual effects, drooling, sweating, diarrhea, nausea, vomiting, and abdominal pain. Neuromuscular symptoms are twitching, weakness, paralysis, and eventually respiratory failure. Symptoms affecting the central nervous system are headache, confusion, depression, convulsions, coma, respiratory depression, and respiratory arrest.

**Treatment of VX poisoning.** Two antidotes exist for VX poisoning: atropine and pralidoxime chloride, also called 2-PAM. Atropine blocks one type of acetylcholine receptor on the post-synaptic nerve cell membrane. This prevents acetylcholine that is in the synaptic cleft from binding to the receptor. Pralidoxime chloride prevents VX from binding to cholinesterase. Together, these drugs have been combined in an antidote kit called Mark I. Mark I is issued to United States troops, in particular those serving in the Persian Gulf region. Diazepam can also be used to treat the seizures and convulsions that may occur as a result of VX poisoning.

If VX is exposed to the eyes, they should be flushed with water for 10 to 15 minutes. Skin contact should be treated with washing in soap and water, 10% sodium carbonate solution or 5% bleach solution. If sweating and muscular twitching occur, then Mark I should be administered. If VX is ingested, Mark I should be injected immediately.

**The history of VX.** VX nerve agent was developed in 1952 by British chemists who were researching different types of insecticides. The United Kingdom traded information about VX with the United States government in exchange for information about thermonuclear weapons in 1953. A program to thoroughly study VX was subsequently begun at the Department of the Army's Edgewood Arsenal in Maryland. In 1957, scientists at Edgewood developed a binary system for delivery of VX in weapons. During the 1960s or 1970s, the Soviet Union's intelligence agencies learned the formula for VX and soviet scientists developed a program for the mass production of VX.

Although VX has not yet been used as a weapon, in 1968, the U.S. Army experimented with open-air tests of weapons containing VX at Dugway Proving Ground near Salt Lake City in Utah. During a test on March 14, a valve failed on an aircraft carrying the nerve gas and 320 gallons of VX were inadvertently sprayed over fields. Subsequently, 6,400 sheep that were grazing in the area died. The Army eventually took responsibility for the mishap and reimbursed ranchers for their loss.

The Iraqi government has admitted to manufacturing VX during the 1990s. It is possible that the formula for

producing VX could have passed to Iraq via Russia, however the U.S. government has found no solid evidence of such a transfer of information. Further, reports surfaced in 2002 that the al-Qaeda terrorist network has obtained VX, but they had not been substantiated as of early 2003.

**The use of VX as a weapon.** VX is an extremely toxic material with low volatility and therefore, it dissipates very slowly. VX also has adhesive properties, which makes it difficult to remove from surfaces. These characteristics make a powerful strategic contaminant. For example, military bases contaminated with VX could result in casualties for several weeks if the base continued to be used. In order to counter such tactics by terrorist groups, scientists at the Department of Energy's Idaho National Engineering and Environmental Laboratory have recently developed technology to detect VX and to predict its degradation rate on concrete surfaces. Because of its potent toxicity, if VX were used on a missile, it could be an extremely deadly weapon. The LD50, or lethal dose for at least 50% of those exposed to VX is 10 ml. Therefore, VX is considered a weapon of mass destruction.

#### ■ FURTHER READING:

##### BOOKS:

- Haugen, David M., editor. *Biological and Chemical Weapons*. San Diego: Greenhaven Press, Inc., 2001.
- Seagrave, Sterling. *Yellow Rain: A Journey through the Terror of Chemical Warfare*. New York: M. Evans and Company, Inc., 1981.
- Sifton, David W., editor. *PDR Guide to Biological and Chemical Warfare Response*. Montvale, NJ: Thompson/Physician's Desk Reference, 2002.
- Wise, David. *Cassidy's Run: The Secret Spy War over Nerve Gas*. New York: Random House, Inc., 2000.

##### ELECTRONIC:

- Chemical Weapons: Nerve Agents. <<http://faculty.washington.edu/chudler/weap.html>> (February 11, 2003).
- Material Safety Data Sheet: Lethal Nerve Agent VX. <<http://www.ilpi.com/msds/vx.html>> (February 11, 2003).
- United States Army. Chemical Agent Fact Sheet: VX. <<http://www.sbcom.army.mil/services/edu/vx.htm>> (February 11, 2003).

##### SEE ALSO

*Chemical Warfare  
Toxins*



*This page intentionally left blank*



## Walker Family Spy Ring

John Anthony Walker, a United States citizen, successfully spied on behalf of the Soviet KGB from 1967 to 1985. Walker employed friends and members of his family in the business of espionage, stealing secrets from U.S. Naval Intelligence and selling them to Soviet agents. During the course of his career, Walker compromised United States military communications ciphers, copied blueprints of Naval vessels and weapons, and stole secret documents.

In 1984, Walker's ex-wife, Barbara Crowley Walker, tipped FBI investigators to her husband's dealings with the Soviets. She told investigators that she suspected he did not work alone, and most likely relied on his brothers and a friend to steal government secrets.

The FBI conducted extensive surveillance of Walker for several months, trying to catch him in the act of leaving information at pre-arranged dead drop for a Soviet agent to retrieve. In April 1985, investigators learned of Walker's plans to leave documents at a dead drop site in Maryland, in exchange for a sizable cash payment to be picked up from another location. On May 19, 1985, FBI agents watched Walker leave a crumpled paper sack near a roadside utility pole. After Walker left the site to drive one hour north to receive his payment, agents seized the dead drop materials, 129 top secret Navy intelligence documents.

Walker then went to the second site to pick up the dead drop a Soviet agent left for him, \$200,000 in cash. However, the bag containing the money was not at the site. After searching for nearly two hours, Walker left the drop site and checked into a local motel, worried that the FBI may have compromised the transaction. Walker was arrested outside his hotel room later the same night.

Despite warnings from his handlers in the KGB, Walker included personal letters and information in his last few dead drops. When the FBI seized Walker's last drop, the package contained not only the stolen secret documents

but also a letter containing the names of other members of his spy ring. The names appeared in code, but FBI and CIA personnel readily identified the cryptonym. Walker's own writing implicated his son, Michael Lance Walker, a seaman stationed aboard the USS *Nimitz*. Michael Walker supplied his father with many of the documents, photographs, and code information that his father sold to Soviet agents. All 129 stolen documents in Walker's final dead drop were stolen by his son.

Walker's letters also noted the involvement of his older brother, Arthur Walker, in the activities of the spy ring. Arthur was a Navy veteran and a defense contractor, privy to information about weapons systems and ship and aircraft design.

Jerry Alfred Whitworth, Walker's best friend and a Navy communications specialist, operated in the spy ring for over ten years. Whitworth supplied Walker with most of the United States cipher and code information leaked to the Soviets.

Walker, his son, and Whitworth were tried on charges of espionage. Walker received life in prison, while Michael and Whitworth received lesser sentences. Walker's son, Michael, was released from prison in 2000.

Although Moscow celebrated Walker as one of their best recruits, Walker's arrest served as a catalyst for a widespread investigation of security procedures within the United States intelligence community. A year after Walker's arrest, investigators and intelligence officials exposed seven other suspected double agents operating against the United States.

### ■ FURTHER READING:

#### ELECTRONIC:

The Center for Counterintelligence and Security Studies.  
<<http://www.cicentre.com>> (April 2003).

#### SEE ALSO

*Ames (Aldrich H.) Espionage Case*

*Dead Drop Spike*  
*Dead-Letter Box*  
*FBI (United States Federal Bureau of Investigation)*  
*Hanssen (Robert) Espionage Case*  
*KGB (Komitet Gosudarstvennoi Bezopasnosti, USSR Committee of State Security)*  
*Russia, Intelligence and Security*

## War of 1812

■ ADRIENNE WILMOTH LERNER

The War of 1812, spawned by the European Napoleonic Wars, was the last war in which the fledgling United States fought its former colonial power, Great Britain. After three years of fighting on land and at sea, the United States military successfully drove the British forces from United States soil, but not before British troops burned Washington, D.C. The War of 1812 assured the United States the independent sovereignty it claimed after victory in the American Revolution and shaped American foreign policy for over a century.

When continental Europe erupted in conflict in 1793, the United States declared itself neutral. Not wanting to anger France or Britain, the two main rivals in the European war, the United States tried to remain out of contentious European politics, especially in regards to European colonial holdings in the Americas. Relations were further strained by British resentment of ongoing United States trade and diplomatic cooperation with France. British ships blockaded United States ports, hoping to prevent supplies and trade goods from reaching France. United States leaders, George Washington and John Adams, worked to ease tensions and lift the blockade, and by 1795, the nation again conducted trade with allies in Europe. However, by 1803, the United States government grew deeply concerned about the presence of a strong British military force in the Great Lakes region. Negotiations with Britain to reduce their military presence in the West and along the northern border of New England failed. Tensions again mounted when France sold the United States significant territories, including the Mississippi River, in the Louisiana Purchase.

In 1805, the British Navy resumed its blockade of the United States coast, prohibiting the export of most goods to continental Europe. The Orders in Council of 1807 further restricted neutral trade with Europe, and authorized British ships to take both the cargo and crew of seized neutral ships. The practice of impressment, forcing captured seamen into service on British ships, inflamed anti-British sentiment in the United States. The passage of the Embargo Act, confining all United States trade to the North American coast, the failure of continued diplomatic relations, and British-incited Indian attacks on United States outposts, gave credence to the opinions of the “War

Hawks” in the United States government. In June 1812, the United States declared war on Britain.

The War of 1812 forced the United States to rapidly form and train military forces. After the Revolutionary War, the federal government only reluctantly allowed provisions for national forces. Most armies were maintained by individual states, with little standardization of training and equipment. The war spanned the entire breadth of the United States and its territories, from the Great Lakes region to New Orleans, Louisiana. Regional armies facilitated troop movement and deployment, but the lack of national infrastructure made travel and communication among the different battlefronts difficult. Military generals attempted to create a complex communication and espionage network, utilizing couriers on horseback and semaphore, to deliver messages. Codes were primitive and easy to break, but both British and American forces employed invisible inks to help conceal communications.

The vast expanses of rough and unfamiliar territory that both armies traversed required the extensive use of scouts. Both British and American forces preferred to use Indian scouts, who often had superior knowledge of regional terrain and could communicate in several indigenous languages. Indian scouts also aided in the recruitment of Indians to fight rival forces. British and United States military leaders also attempted to spark warfare between rival tribes with varying allegiances, hoping to distract opposing forces or break their aid network. Extensive contact with indigenous populations proved devastating, as during the American Revolution, disease ravaged Indian villages and several thousand Indian warriors died in battle.

From 1812 to 1814, the United States suffered numerous crushing defeats at the hands of superior British forces. United States offensives failed to take the Great Lakes region, and military defenses could not keep British troops from occupying Washington, D.C. Anticipated French aid never materialized in the 1813, as the tide of war in Europe had shifted decisively in favor of the British, and Napoleon’s French Empire was in grave danger of collapse. American diplomats in Paris maintained a small espionage network in Europe and the Americas to monitor the British military and diplomatic corps. A French spy, posing as a local trader, rode to the White House to inform the president and cabinet members of the British plans to invade, occupy, and then destroy Washington, D.C. The government fled the British invasion of the capital city, but only by a matter of hours.

Despite the grim prospects of the United States land campaign in the early years of the war, the new United States Navy mounted surprisingly successful battles against the powerful British Navy. The United States reluctantly formed its Navy to combat the extortionist trade monopoly of the North African Barbary Pirates who dominated shipping in the Mediterranean. While wealthier European government simply paid annual tributes and occasional ransoms to the Barbary authorities, the fledgling United States Federal government could not afford to pay such

large sums of money. The nation mounted a small but highly effective Navy, eventually driving the Barbary authorities to capitulation. After the conflict, the government only narrowly voted to keep naval forces.

When the British began the blockade of the American coastline, United States navy and merchant ships successfully ran the blockade. The government employed “pirate” ships to destroy British ships, and recapture seized cargo and Americans impressed into service. With the outbreak of war, naval resources were increasingly devoted to strategic sea campaigns against British vessels. The United States Navy successfully captured the British frigate *Macedonian*, defeated the *Java*, and raided several other merchant and military ships. Victories at sea, though limited, enforced the need for a permanent navy in the United States and ensured its continued survival. One hundred and forty years later, the United States Navy surpassed the British fleet to become the world’s dominant sea power.

As the French were defeated in Europe, the British devoted more resources to the battlefield in America. However, United States forces rallied, turning the tide of the war in their favor by August 1814. Wishing to avoid clear military defeat, both sides began peace negotiations. The British failure to capture Baltimore prompted the government to settle their dispute with the United States, instead of continuing a lingering, expensive, and increasingly stalemated overseas war. The Treaty of Ghent formally ended the war in 1815. On January 8, 1815, after the signing of the treaty, United States forces, commanded by Andrew Jackson, achieved a stunning victory against the British at the port of New Orleans. Since communication was tedious across the Atlantic and the expansive western territory of Louisiana, news of the Treaty of Ghent did not reach either forces in time to prevent the engagement. The Battle of New Orleans gave the impression that the long-stalemated war was a sound United States victory, but the new nation was successful largely because of the failure of British offensive operations.

After the War of 1812, the United States declared firmer international policy. With the issuance of the Monroe Doctrine in 1823, the nation stated its policy of non-intervention in European conflicts. Furthermore, the United States declared the New World closed to further colonization, and that attempts of foreign powers to intervene in conflicts between colonial powers and their colonies would be viewed as an act of aggression. The War of 1812 solidified the political and military preeminence of the United States in the Americas, and began the great expansion westward toward the Pacific coast.

#### ■ FURTHER READING:

##### BOOKS:

Dudley, Wade G. *Splintering the Wooden Wall: The British Blockade of the United States, 1812–1815*, reprint ed. Annapolis, MD: U.S. Naval Institute, 2000.

Hickey, Donald R. *The War of 1812: A Forgotten Conflict*. reprint ed. Champaign, IL: University of Illinois Press, 1990.

Katcher, Philip R. *The American War, 1812–1814 (Men-at-Arms, no. 226)*. reprint ed. Buffalo, MN: Osprey Publishing, 1990.

#### SEE ALSO

*Revolutionary War, Espionage and Intelligence*

## Water Supply: Counter-Terrorism

■ BRIAN HOYLE

The water supply in many communities in the developed world comes from a surface water source such as a lake. Water can also be pumped from aquifer located underground. Typically, the water is routed to a treatment plant, where a variety of physical and chemical processes render the water safe to drink. The “finished” water is then pumped through pipes (i.e., the distribution system) to the consumer’s taps.

For over a century this process has been geared toward providing high quality water, without consideration of the security of the acquisition, treatment, and distribution of water. However, particularly since the 1990s, the threat of a deliberate contamination of water supplies has become more probable.

In the wake of the September 11, 2001 terrorist attacks on the World Trade Center and the Pentagon in the United States, surface water supplies, water treatment plants, and distribution systems were quickly recognized as potential targets of a terrorist attack. While water facilities are often equipped to discourage mischief (i.e., a chain link fence surrounding a reservoir), virtually no water facilities are designed to prevent a deliberate and coordinated attack.

Many compounds dissolve in water and microorganisms are so small that, for example, up to 6 million bacteria need to be present in each milliliter of water before the water will appear less than crystal clear. Thus, the addition of a lethal quantity of a potent poison or disease-causing microorganism to a water supply could be done without attracting undue notice.

During the 1990s, and especially since the events of September 11, 2001, efforts to develop effective strategies to counter a terrorist attack on water supplies have been widely debated.

The fact that major urban systems need to supply huge quantities of drinking water every day could already be a counter-terrorist strategy. Even given the ease by

which a reservoir could be contaminated, the large volume of the water reservoirs of major urban centers would dilute the added poison to very low levels. A lethal dose of a poison at the consumer's tap would require the addition of a huge amount of the contaminant. For example, it has been estimated over 400,000 metric tons of hydrogen cyanide would have to be added to the Crystal Springs Reservoir—a major reservoir for the city of San Francisco—to supply enough poison to kill or debilitate someone drinking one glass of water from the reservoir.

However, smaller reservoirs are at risk, as are smaller water tanks. Increased security at treatment plants would be an effective deterrent to sabotage. However, such security would be expensive and the cost would be passed to the consumer.

In most municipalities, water treatment involves the addition of chlorine or chlorine products to kill microorganisms. The deliberate disabling of the chlorination system of a treatment plant would make contamination of the drinking water a certainty. For example, a breakdown in the chlorination of the drinking water of Walkerton, Ontario, coincident with the run-off from a cattle field that contaminated the water supply with *Escherichia coli* O157:H7, sickened over 2,000 people and killed at seven people in the summer of 2000.

Even a secure treatment facility supplying chlorinated water is no guarantee of safe water. Recent history has shown that chlorinated water is susceptible to contamination by microorganisms that are resistant to the chemical. Specifically, the protozoa called *Giardia* and *Cryptosporidium* have a spore-like stage in their life cycles that survives exposure to chlorine. A *Cryptosporidium* contamination of the water supply of Milwaukee, Wisconsin, sickened over 200,000 people and killed almost 100 people.

While illness outbreaks with the protozoa have so far been accidental, the use of the microorganisms as a weapon is conceivable. In the United States, municipalities have been legislated to provide alternate means of dealing with drinking water to counter the threat posed by *Giardia* and *Cryptosporidium*. This legislation has been prompted by health concerns. Nonetheless, it will prove to be a counter-terrorism measure.

The distribution system that carries water from the treatment plant to the consumer's taps is another potential target of terrorism. The high pressure inside the pipes would make the introduction of a contaminant difficult. However, the lack of security along the distribution system could enable a dedicated group to commission the digging equipment needed to uncover a pipe and stop water flow long enough to contaminate the water.

Patrolling a distribution system is impossible. For now, the most effective counter-terrorism strategy is to make manholes and storage tanks inaccessible.

Another microbial terrorist threat to drinking water is *Bacillus anthracis*. This bacterium, which is the cause of anthrax, can form a very hardy structure known as a spore.

Studies have determined that the spore form can survive in chlorinated water for at least two years. If ingested in a glass of drinking water, or inhaled in the humid environment of a shower or bath, the spores can revive, and the growing bacteria can cause the disease.

Other chlorine-resistant microorganisms that have been identified as bioterrorism agents include *Clostridium perfringens*, *Yersinia pestis* (the cause of plague), and biotoxins (e.g., aflatoxin and ricin).

Countering the deliberate use of such microorganisms will necessitate the rapid detection of even tiny quantities of the microorganisms or their toxic products. Use of rapid detection devices in an early warning system would be an effective counter-terrorism strategy, albeit one that would require dedicated personnel or hardware to monitor the water system.

One promising technology is the use of an electronic sensor ("the electronic nose") to detect chemicals. This method has been successful in detecting spoilage and disease causing bacteria present on fruit by virtue of the unique chemical compounds given off by the bacteria. However, the electronic nose would have to be adapted for use with water.

A detection method that already successfully detects and identifies bacteria such as *Escherichia coli* in fresh water relies on the binding of fluorescent antibodies to the surface of the bacteria and the detection of the bound antibodies by the resulting fluorescence. A prototype of the device is portable and so can be taken to hydrants for the testing of water throughout a distribution system. When in production within the next several years, the device will offer a means of rapidly monitoring water for contaminants.

Another promising technology relies on the recovery of genetic material (deoxyribonucleic acid; DNA) from the sample, and the detection of sequences of the DNA that are unique to the target bacteria by the use of a mirror image piece of DNA that will selectively bind to the target sequence. DNA microchips utilize this technique to detect bacteria from samples as complex as soil and ocean water.

Thus, there is potential for the development of rapid tests to detect bacterial contamination of drinking water. Whether the benefits of implementing an early warning system of chemical and microorganism detection will justify the costs remain to be determined.

In the short term, the best counter-terrorism strategy for many water systems will continue to involve a survey of the system in order to identify points where the system is vulnerable (i.e., unlocked hydrants) and taking action to secure those points (i.e., locking hydrants). As well, public notification of water contamination, and response of authorities (e.g., police, fire department, and medical personnel) to a contamination should be an integral part of a community's emergency response plan.

Despite the vulnerability of water to deliberate contamination, the reality continues to be that the probability of such action is very low. A terrorist can deliver a lethal

payload by air or through routes like the postal system more easily and using less microorganisms than would be required for the contamination of a water supply.

#### ■ FURTHER READING:

##### BOOKS:

Lesser, Ian O., and Bruce Hoffman. *Countering the New Terrorism*. Santa Monica: Rand Publications, 1999.

##### PERIODICALS:

Betts, K. S. "DNA chip technology could Revolutionize Water Testing." *Environmental Science and Technology* no. 33 (1999): 300A-301A.

Burrows, W. D., and S. E. Renner. "Biological Warfare Agents as Threats to Potable Water." *Environmental Health Perspectives* no. 107 (1999): 975-84.

Foran, J. A., and T. M. Brosnan. "Early Warning Systems for Hazardous Biological Agents in Potable Water." *Environmental Health Perspectives* no. 108 (2000): 993-96.

Weckerle, J. F. "Domestic preparedness for events involving weapons of mass destruction." *Journal of the American Medical Association* no. 283 (1997): 435-38.

##### SEE ALSO

*Biological Warfare*  
*Chemical Warfare*  
*Pathogen Transmission*  
*United States, Counter-terrorism Policy*

## Watergate

#### ■ ADRIENNE WILMOTH LERNER

Five men, known as the "White House plumbers," broke into the Watergate apartment and office complex on June 17, 1972. The well-trained burglars' mission was to raid Democratic Party offices in the complex and obtain secret documents pertaining to the presidential election. The five men, Frank Sturgis, Bernard Baker, Eugenio Martinez, Virgilio Gonzalez, and James McCord were caught and arrested. Subsequent investigations revealed the involvement of E. Howard Hunt and G. Gordon Liddy in planning the break-in, and possible connections to the White House and Central Intelligence Agency (CIA).

Three of the "White House plumbers," Liddy, McCord, and Hunt were former members of the CIA. When investigations revealed that the burglars used sophisticated eavesdropping and espionage equipment, the scandal grew to encompass the United States intelligence community. Eavesdropping devices, including wiretaps and tape recorders, were planted in the target Watergate offices before the break-in to monitor communications. During the burglary, the men used miniature cameras, complex lock

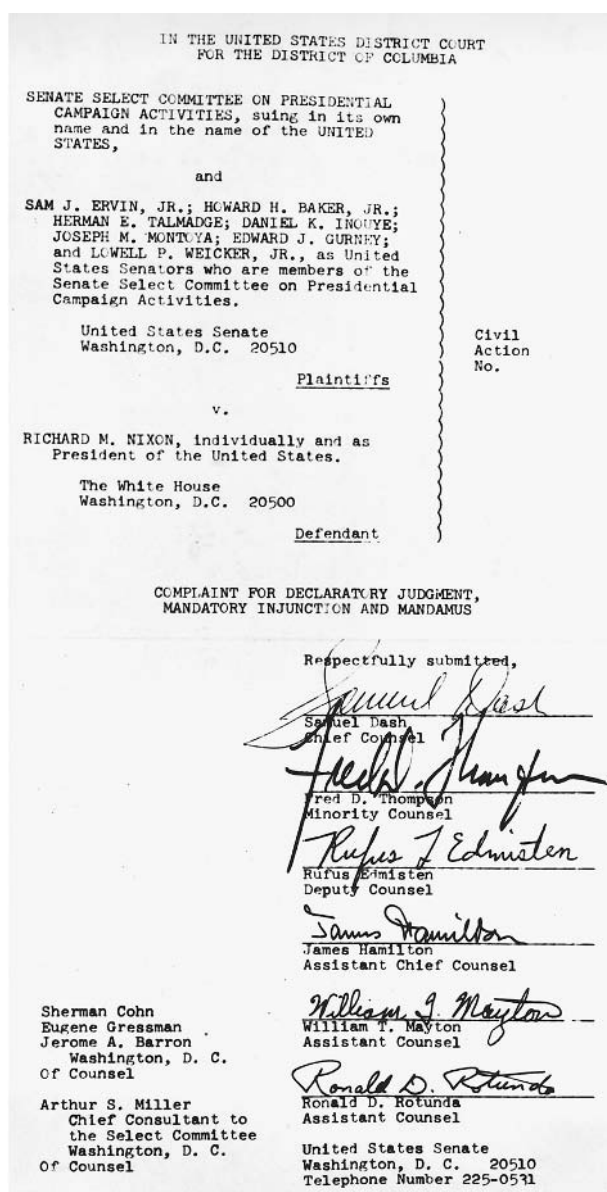


Photo showing the first and last pages of the complaint filed in Washington, D.C., by the Senate Watergate committee in 1973 naming as defendant Richard Nixon both individually and as president of the United States. AP/WIDE WORLD PHOTOS.

picks, and military issue walkie-talkies. Authorities discovered small canisters of tear gas on two of the men. Some of the tools were even marked with government identification numbers, evidence that the operation was planned or authorized by a member of the government. The White House, and President Richard Nixon himself, were soon implicated, elevating the Watergate incident to full-fledged political scandal at the highest political level.

The men involved in the Watergate affair were members of the Committee to Re-elect the President sometimes referred to colloquially as "CREEP." Months before

the break-in, members of CREEP advised President Nixon to develop “political intelligence capabilities” to further his campaign. Facing public backlash from the war in Vietnam, Nixon’s committee sought to discredit Democratic opponents in an attempt to gain ground in the election. Following the Watergate burglary, and the arrest of the “White House plumbers,” Federal authorities conducted a full investigation of the incident. The White House, and CREEP, attempted to block full disclosure of the scandal.

The cover-up of the Watergate affair was itself a deft intelligence maneuver. Members of CREEP destroyed pertinent documents and encouraged allies in the United States intelligence community to do the same. The Nixon White House destroyed tape archives of phone conversations. FBI Acting Director Patrick Gray later resigned his post after admitting to destroying Watergate documents at the request of CREEP officials. Those in custody gave a series of false statements, committing perjury, in an attempt to distance the scandal from the Nixon administration. As a result, only three of the original eight men arrested were indicted. For a while, the cover-up was successful.

Following Nixon’s re-election, the U.S. Senate began a formal inquiry of the Watergate scandal. The previous CIA and FBI investigations failed to implicate the Office of the President because none of the persons questioned mentioned the involvement of the White House in CREEP operations. In March 1973, Hunt asked for a significant sum of “hush money” to refrain from going to the FBI or Senate committee with information about the scandal. He received \$75,000.

Most of those involved in the scandal decided to exercise their Fifth Amendment rights and not testify to the Senate committee. Nixon announced a new investigation of the scandal on March 21, 1973, but immediately began to stonewall the process. A letter from McCord to Judge Sirica on March 23 formally implicated the White House plumbers, CREEP, and the president in the Watergate scandal. The cover-up fell apart, and a desperate administration resorted to a series of “dirty tricks” to shift the focus of the investigation away from the Nixon administration.

The “dirty tricks” focused on discrediting those who testified against CREEP, White House, and intelligence agencies. Some were accused of sexual misconduct, others of financial irregularities. Stink bombs were planted in offices. However, the most devious trick was the falsification of State Department cables by Hunt to implicate former President John Kennedy in the assassination of the South Vietnamese President Diem. Hunt tried to sell the cables to the media, in an attempt to anger and influence predominantly Democratic Catholic voters. The timely surfacing of the mysterious cables, as well as public disclosure of campaign finance irregularities by the Nixon administration further fueled the scandal.

While the break-in itself was an illegal act, the Watergate scandal had far greater legal consequences. The involvement of former CIA members raised questions about the prevalence of political espionage in the United States government. Using the resources of the intelligence for political espionage or personal gain is strictly illegal under American law. In addition, the involvement of the White House implied the Office of the President resorted to gross abuses of its power and authority. Subsequent Senate hearings and FBI investigations reached similar conclusions, and nearly 30 people in the Nixon administration were fined or imprisoned.

Complex intelligence operations and sophisticated equipment had permitted the “White House plumbers,” CREEP, and Nixon to perpetrate and hide many of their crimes. However, the same sophistication of cloak and dagger operations ultimately undid the Nixon administration and broke the mysteries of the Watergate scandal. Nixon recorded most conversations in his office. An intense legal battle, eventually reaching the Supreme Court, ensued over the tapes, their possible editing, and their admissibility in Senate Select Committee hearings. Facing impeachment after the subpoena of the tapes, Nixon resigned his office. Although he was later pardoned by President Gerald Ford, some of the people involved in the scandal served long prison terms, never breaking their cover story in relation to the scandal.

The most important political scandal in U.S. history was perhaps best put in perspective by the late comedian Bob Hope, who said of Watergate, “It gave dirty politics a bad name.”

#### ■ FURTHER READING:

##### BOOKS:

- Bernstein, Carl, and Bob Woodward. *All the President’s Men, 25th Anniversary Edition*. New York: Simon and Schuster, 1999.
- Kurland, Philip B. *Watergate and the Constitution (The William R. Kenan, Jr., Inaugural Lectures)*. Chicago: University of Chicago Press, 1978.
- Kutler, Stanley I. *The Wars of Watergate: The Last Crisis of Richard Nixon*. New York: W.W. Norton and Company, 1992.

##### ELECTRONIC:

- United States National Archives and Records Administration. Watergate resources. <[http://www.archives.gov/digital\\_classroom/lessons/watergate\\_and\\_constitution/teaching\\_activities.html](http://www.archives.gov/digital_classroom/lessons/watergate_and_constitution/teaching_activities.html)>(01 December 2002).

##### SEE ALSO

- Church Committee*  
*Vietnam War*

## Weapon-Grade Plutonium and Uranium, Tracking

■ K. LEE LERNER/LARRY GILMAN

Weapon-grade (or “bomb-grade”) uranium or plutonium is any alloy or oxide compound that contains enough of certain isotopes of these elements to serve as the active ingredient in a nuclear weapon. Some civilian weapon-grade materials are tracked by international organizations, especially the United Nations’ International Atomic Energy Agency (IAEA) and the European Atomic Energy Community (EURATOM), to prevent their diversion to bombs. The goal is to prevent nuclear proliferation, that is, the possession of nuclear weapons by more and more groups.

IAEA safeguards track weapon-grade materials (or, in the case of plutonium, dilute materials that could be refined to weapons grade) in non-military nuclear fuel cycles in states that are signatories to the Non-Proliferation Treaty (NPT) of 1968. Those states that already had nuclear weapons at the time of the treaty’s creation—the U.S., United Kingdom, France, Russia, and China—are not subject to IAEA safeguards. Only four states—Cuba, India, Israel, and Pakistan—have not signed the NPT and are not part of any international safeguard system. Of these four, all have nuclear weapons except Cuba, which western intelligence agencies assert is not currently seeking nuclear weapons. EURATOM safeguards civil plutonium and uranium in the European countries, including materials not covered by mandatory IAEA safeguards under the NPT (i.e., those in the UK and France). The IAEA and EURATOM cooperatively safeguard European materials to avoid redundancy.

Military nuclear materials are tracked not by the IAEA but by the governments that own them. Because the tracking techniques employed internally by nuclear-weapons states vary from nation to nation and are always partly or wholly secret, and since EURATOM safeguards are essentially the same as IAEA safeguards, this article restricts itself to IAEA safeguards on nuclear materials in the 182 non-nuclear-weapons signatories of the NPT.

### Definition of “Weapon-Grade”

“Weapon-grade” uranium or plutonium is sometimes defined as any alloys pure enough to be used in bombs by governments building light-weight nuclear weapons for carriage in missiles, artillery shells, or other delivery systems. The highly-enriched uranium (HEU) preferred by professional weapons designers is more than 90% uranium-235 ( $^{235}\text{U}$ ), and the enriched plutonium used for such purposes is nearly pure metal. However, “weapon-grade” it is more usefully, and more commonly, defined as any

material pure enough to serve in a nuclear weapon, regardless of that weapon’s efficiency or elegance of design. Uranium enriched to only about 50%  $^{235}\text{U}$ , and probably less, can be used to make a crude nuclear bomb, and it is possible to make a bomb from material that is only 15–25% plutonium (e.g., mixed-oxide fast breeder reactor fuel). A “crude” bomb would probably have an explosive force of several tens of kilotons (where one kiloton equals the explosive force of one thousand tons of trinitrotoluene, TNT), comparable to the bombs that destroyed Hiroshima and Nagasaki in 1945.

Weapon-grade fissile materials are not found in nature, but must be produced.  $^{235}\text{U}$  is found only in dilute form in nature. It constitutes about .71% of the uranium in ore, the rest being mostly the isotope  $^{238}\text{U}$ , which is not fissile enough to be a reactor fuel or bomb material. Reactor-grade uranium (i.e., the fuel for civilian nuclear power plants, which is about 3%  $^{235}\text{U}$ ) and weapon-grade uranium are obtained by enriching the concentration of  $^{235}\text{U}$  in metal extracted from ore, a complex and expensive industrial process. The nearly pure  $^{238}\text{U}$  that is left over from enrichment, although useless as a fuel or explosive, can be partly transformed into plutonium by neutron bombardment in a particle accelerator or nuclear reactor. (There are several isotopes of plutonium, not all equally suitable for bombs, but because all readily available isotopic blends of plutonium are suitable for bomb-making, this article refers simply to “plutonium.”)

These facts are important to the tracking or safeguarding of weapon-grade material. Since  $^{235}\text{U}$  exists in nature and only needs to be concentrated to become a bomb material, an ideal tracking system for would station observers at every stage of uranium extraction and refinement, from the mine to the enrichment plant. This would cost too much, so the IAEA monitors selected industrial processes, namely enrichment plants, fuel-fabrication facilities, and reprocessing facilities. A reprocessing facility is a factory where nuclear-reactor fuel that has been isotopically altered by irradiation in a reactor core and is no longer isotopically optimal for fuel purposes (“spent” fuel) is dissolved in acid and its  $^{235}\text{U}$  and plutonium separated out. (What is left is high-level nuclear waste.) Reprocessing is the sole source of weapon-grade plutonium, as plutonium occurs in nature only in trace amounts; therefore, IAEA safeguards track not only separated plutonium but spent nuclear fuel.

### The Safeguarding Task

There are three basic stocks or inventories of weapon-grade (or pre-weapon-grade) material: military inventories, transitional inventories, and civil inventories. *Military inventories* consist of fissile materials (almost entirely alloys of uranium and plutonium) that are already built into weapons, are stockpiled for possible weapons use, or are stockpiled for or already used in naval reactors. (Due to size constraints, the reactors used to drive some submarines and military surface ships require weapon-grade



uranium as fuel). *Transitional inventories* consist of materials that have been removed from weapons or declared by the states that own them to be in excess of their weapon-making needs. By far the largest transitional stockpile in the world is that of Russia, nuclear inheritor state of the Soviet Union. *Civil inventories* consist of materials belonging to the nuclear-power fuel cycle, including stockpiled HEU and plutonium separated from spent fuel, plutonium and HEU loaded or stockpiled as fuel for specialized reactors (e.g., fast breeders), and plutonium and HEU in spent reactor fuel of all types. The basic goal of international safeguards is to track materials in the transitional and civil inventories to prevent them from being secretly diverted to weapons by terrorists or governments. (Although the transitional inventories are held by nuclear-weapon states not required by the NPT to submit them to IAEA safeguards, some of them, notably Russia's, are voluntarily submitted to IAEA safeguards.)

About 3,000 tons of plutonium and HEU have been produced by the civil and nuclear military facilities to date, with hundreds of kilograms of new plutonium forming constantly in the fuel rods of nuclear reactors worldwide. About 700 of these tons are in military inventories, about 1,300 tons in transitional inventories (mostly in the U.S. and Russia), and about 1,000 tons in civil inventories. Because the civil inventories in some of the largest nuclear-power states (i.e., the U.S., U.K., France, and Russia) are not subject to IAEA safeguards, only about 24 tons of weapon-grade plutonium and uranium—less than 1% of the world stock of these materials—is safeguarded. Though apparently small, this quantity of material could produce hundreds of nuclear weapons, and is exactly that fraction of the world's HEU and plutonium inventory that is most vulnerable to diversion. The IAEA, like a border patrol, thus deploys its forces along a critical edge rather than spreading them over the domain of all weapons-grade materials.

Safeguards are designed to deter—by making it difficult to conceal—any attempt to concentrate non-weapon-grade nuclear material into weapon-grade material or, alternatively, to divert weapon-grade material from peaceful purposes (e.g., breeder-reactor fuel) to weapons. Safeguards are thus after-the-fact measures designed to detect a material diversion that has already occurred, quickly enough to detect the diversion before a nuclear weapon can be assembled.

## Methods

The two basic methods used to track weapons-grade nuclear material are accountancy and physical inspection.

**Accountancy.** The NPT requires every signatory nation to “establish and maintain [its own] system of accounting for all nuclear material subject to safeguards,” that is, HEU

and plutonium. In other words, the IAEA seeks to build on national accounting controls rather than building its own system from scratch. (It does so not because national controls are intrinsically better, but to control costs.) The IAEA specifies, in part, what these national accounting procedures shall be, in order to assure that their adequacy and compatibility with the IAEA's own methods.

In this context, a “system of accounting” means a system of inventorying, similar in principle to that used to run a grocery store. The IAEA defines “material balance areas,” specific physical zones which may be as large as entire facility or as small as a single room, for which inventories must be kept. Whenever safeguarded materials are brought in or out of a material balance area, records must be made of the amounts, entering, leaving, and in the material balance area. If the totals do not add up, a diversion is suspected.

**Inspection.** The fact that a nation is responsible for inventorying its own nuclear materials creates an obvious opportunity for cheating: a state might simply fabricate records that show no diversions. To prevent this, the IAEA analyzes each nation's records for inconsistency or other signs of fraud. More importantly, it conducts on-site inspections. Formerly, inspection consisted mostly of visits by IAEA personnel. Site visits by inspectors remain essential, but with the development of new detection technologies and computer systems, automatic or “unattended” safeguards have become more widely used. For example, all entry points to a material balance area might be recorded continually on sealed videotapes that are later analyzed by the IAEA for suspicious activity. Sensors that detect the presence, type, and quantity of nuclear materials by measuring neutrons, alpha particles, or gamma rays can be located at the access gate of a reprocessing plant, near a fuel-storage area, or in other key locations. (Inspections or video monitoring would assure that temporary exits are not being cut in the perimeter fence elsewhere, to escape surveillance.) The efficacy of inspection is increased by requiring that the NPT signatory state whose materials are being safeguarded submit information about the design of its nuclear facilities to the IAEA. The IAEA may also place special seals on containers of safeguarded material, then re-inspect periodically to verify that the seal has not been broken, and require that an inspector be present if the seal is to be broken. The purpose of inspections is, in short, not to directly track all flows of safeguarded material, but to keep the inventory system honest.

**Measurement inaccuracy.** All the measurement processes involved in tracking HEU and plutonium have built-in error. If, for example, a particular scale is only accurate to within a milligram, then there is always 1 mg of uncertainty about how much HEU or plutonium is resting on it. If

a sample of HEU or plutonium that is known to have a mass of 1.00 g is broken in two and each piece measured on a scale having 1-mg inaccuracy, and if these two measurements both read .499 g (for a total of .998 g), it is impossible to tell whether .002 g of controlled material has been diverted or the numbers merely reflect random measurement error. To combat this source of uncertainty it is possible to screen for “systematic” errors, that is, errors that trend systematically in some direction; in particular, errors that always show a loss of material rather than a gain would be more suspicious. (Truly random error should sometimes show too much, rather than too little, material.) However, clever manipulation of error margins inside a complicated system could pit false gains against real losses, thus preventing the appearance of systematic error and concealing small, persistent diversions.

In reprocessing facilities, which extract HEU and plutonium from spent fuel, this problem is particularly acute, as a material balance can only be performed on each batch of liquid material processed by the plant. Cumulative material-balance inaccuracies of up to 1% are probably unavoidable in reprocessing. In a reprocessing facility such as the U.K.’s Barnwell, which was originally designed to extract 15 tons of plutonium per year from 1500 tons of spent fuel, this would mean that 150 kg of plutonium could be diverted undetectably from the plant every year—enough for about 15 atomic bombs. The IAEA Safeguards Division seeks to track inventories in individual states to within 8 kg of plutonium and 25 kg of HEU annually—enough to easily build a single bomb. However, if a state was willing to wait a few years for each bomb, its diversions could remain within the intrinsic error limits.

**Strengthened safeguards.** In the early 1990s, IAEA inspectors discovered that Iraq, though a signatory of the NPT and subject to the full range of IAEA safeguards, had for years been conducting a covert nuclear-weapons program involving thousands of personnel, mostly at facilities already subject to IAEA inspection. It was the first serious attempt by an NPT signatory state to circumvent IAEA safeguards, and was partly successful. Judged by its ultimate goal, however—to produce nuclear weapons—it was an apparent failure; given information by U.S. and U.K. intelligence agencies, IAEA inspectors finally became suspicious and detected the fraud. IAEA inspectors asserted that Iraq (prior to the 2003 American-led war to disarm Iraq) had not been able to reconstitute its nuclear weapons program. In any case, the incident proved that existing IAEA safeguard standards were inadequate. These have been replaced by what the IAEA terms the “strengthened international safeguards system,” which includes stricter and more thorough inventorying; greater access to information about reactor-facility designs, uranium mines, and uranium concentration plants; environmental sampling for signs of radioactivity; more complete facility access; and surprise inspections.

## ■ FURTHER READING:

### BOOKS:

- Arlt, R., et al. “Use of CdZnTe Detectors in Hand-Held and Portable Isotope Identifiers to Detect Illicit Trafficking of Nuclear Material and Radioactive Sources.” *Nuclear Science Symposium Conference Record*, Vol. 1, IEEE, 2001: 4–18; 4–23.
- Koster, J. E., et al. “Alpha Detection as a Probe for Counter Proliferation.” 28th Annual International Carnahan Conference on Security Technology, 12–14 Oct. 1994, IEEE, 1994: 6–19.
- Lovett, James E. *Nuclear Materials: Accountability Management Safeguards*. American Nuclear Society, 1974.
- Mercier, M. T., R. J. Huckins, and G. S. Zalokar. “A Local Data Acquisition Subsystem for Plutonium Safeguards.” *Nuclear Science Symposium and Medical Imaging Conference Record*, 2–9 Nov. 1996, IEEE, 1996: 1254–59.
- Walker, William, and Frans Berkhout. *Fissile Material Stocks: Characteristics, Measures and Policy Options*. New York: United Nations, 1999.
- Willrich, Mason, ed. *International Safeguards and Nuclear Industry*. Baltimore, MD: Johns Hopkins Press, 1973.

### ELECTRONIC:

- International Atomic Energy Agency (IAEA). 2003. <<http://www.iaea.org/worldatom/>> (April 2, 2003).
- Lu, Ming-Shih. “The IAEA Strengthened International Safeguards System.” Brookhaven National Laboratory. 1998. <<http://www.nautilus.org/library/security/papers/LuISODARCO.PDF>> (April 2, 2003).

## Weapons of Mass Destruction

### ■ ALEXANDR IOFFE

The concept of Weapons of Mass Destruction appeared during War World II after the use of atomic bombs. In the mass consciousness, weapons of mass destruction are usually associated first with atomic weapons, although the concept includes certain chemical and biological weapons.

The atomic bomb was used only twice in World War II, in bombarding the Japanese cities of Hiroshima (August 6, 1945) and Nagasaki (August 9, 1945) by the United States. The first bomb employed uranium-235 and produced an explosion equivalent in power to approximately 15 kilotons of TNT gunpowder. The second bomb employed plutonium and was equivalent in power to approximately 21 kilotons of TNT gunpowder.

On August 7, 1945 the General Staff of Japan received an alarming telegram from the Hiroshima region claiming that the city was completely destroyed by one bomb. Approximately 130 thousand people were killed because of the bombardments of both cities, and both Hiroshima and Nagasaki were completely destroyed. The number of

injured also numbered in the hundreds of thousands, and the consequences of burns and radiation were apparent in bombardment victims for many years, often including the next generation.

The process of radioactive isotope (uranium-235 or plutonium-239) fission is the basis of the action of atomic weapons. A mammoth amount of energy is generated in this process. The dissipation of energy in an atomic bomb explosion occurs in the following approximate ratio: bomb blast and wind – 50%; thermal rays – 35%; and (radioactive) radiation – 15%. These are the three main striking factors of an atomic explosion.

An even more powerful weapon, the hydrogen fusion bomb, was created several years after the A-bomb, and was created practically simultaneously in USA and in the former Soviet Union. The power of the H-bomb is hundreds of times higher than the power of an A-bomb. The process of hydrogen isotope fusion is the basis of the thermonuclear weapon action. The start of this reaction, however, must be initiated by a nuclear fission explosion.

On November 1, 1952, a 10.4 megaton thermonuclear explosion code-named MIKE, ushered in the thermonuclear age (it was an explosion of a special model of the device). The island of Elugelab in the Eniwetok Atoll in Pacific was completely vaporized.

The first H-bomb was exploded in the USSR in August, 1953, followed on March, 1, 1954, by the American explosion of a more powerful hydrogen bomb (approximately 15 megatons). The Soviets responded with the most powerful H-bomb explosion yet, in the Soviet Union on October 15, 1961, over the Novaya Zemlya (New Earth) island (in the Polar Ocean) at a height of 4000 meters (approximately 13,000 feet) over the Earth. Its power was almost 50 megatons. A gigantic fireball was created by the explosion that reached to the height of about 67 km (41.5 miles), and its light was seen for a distance of more than 1000 km (621 miles). The explosion also resulted in a blast of wind that was felt for hundreds of kilometers.

The creation of the atomic bomb in the USA during World War II was an exceptional scientific phenomenon. The interval between the discovery of the physical fusion process that is the basis of the weapon action, and the moment of its first test (July 16, 1945, in the New Mexico desert) was only several years, and up to the end of this test, its creators were not absolutely sure that the test would be successful. The United States committed an enormous amount of scientific and monetary resources towards the creation of the atom bomb, and a new branch of industry was formed.

In 1949, the A-bomb was also created in the USSR. Later, a big concern among American intelligence authorities arose about atomic espionage, which helped the Russians to create the A-bomb during such a short period. Several people who passed to the Russians secrets about atomic elaboration were revealed and arrested, including Claus Fuchs and Julius and Ethel Rosenberg. Although some thought that espionage was the crucial factor in the

Russian's success, the main secret was whether the nuclear chain reaction of the A-bomb could be successfully created and controlled. As soon as the bomb exploded over Japan, this secret became clear. Additionally, in 1945, a noted report by American physicist H. D. Smith entitled "*Atomic Energy for Military Purposes*" was openly published, in which the principles of the bomb's action, the methods of isotope separation, and even some of the characteristics of its construction were described in detail. The post-war Soviet Union of 1945 still contained highly qualified scientists, and the totalitarian regime dedicated all possible resources to the high-priority project of atomic bomb development. Thus, the arms race of the 1960s and 1970s has its beginnings as far back as the early post-World War II era.

Many chemical weapons are also considered weapons of mass destruction. Various lethal poisons were known and successfully used in warfare as long ago as ancient times. The creation of such substances for weaponry is much easier and cheaper than, for example, separating uranium isotopes as is necessary for a nuclear weapon. Chlorine gas, for example, one of the simplest poison gases, can be created in small amounts in a simple laboratory. The problem of delivering poison gases to a battlefield is also much simpler than delivering an atomic weapon.

During World War I, the Germans were the first to use poison gases on the modern battlefield. The Germans bombarded their enemies with artillery shells armed with poison gas, or simply ejected gas from their containers. The names of some poison compounds are reminiscent of World War I; for instance, the poison gas yperite (mustard gas) has in its origin the name of the Belgian city Yper, where the gas was used the first time. In 1915, the Germans also conducted massive attacks using chlorine. As a result of one chlorine gas attack, five thousand persons were killed and about ten thousand were injured. The Germans ejected chlorine from 5730 balloons containing about 168 tons of chlorine within the 5 to 8 minute duration of the attack.

Officially, the use of chemical weapons is forbidden by the Hague Conventions concluded in 1899 and 1907, and these resolutions were further clarified and strengthened by the Geneva Protocol of 1925. The first international disarmament treaty that banned the production and stockpiling of biological weapons, and provided for destruction of existing stores became open for signature in 1975. Almost 30 years later, the treaty is still the subject of regular debate and clarification and lacks wide spread ratification.

In the meantime, chemists of various governments have worked actively to create new chemical substances with various destructive factors. Additional chemical weapons have been derived from toxic industrial chemicals that were originally designated for useful purposes, such as pesticides. Chemical weapons can generally be divided among several groups, depending on their action on people, including vesicants, toxins, incapacitating agents, nerve

agents, and irritants. The production of vesicants is not technologically complicated. The production of the nerve agents, however, requires significantly more sophisticated chemical processing. Some production processes require strict temperature control, and containment of the toxic substances and gases can pose problems. Depending on the immediacy of use, purity of the product can add a difficult dimension to production. In some cases, special equipment or handling is required to prevent corrosion of equipment and/or rapid deterioration of the product.

Chemical weapons were not used during World War II, although the main participants had large reserves of such weapons. Production of these weapons continued after World War II, and only recently the USA and Russia have stopped their production and agreed to begin to destroy existing stockpiles. Other nations and extremist groups have recently used chemical weapons. Iraq used chemical weapons during the Iran-Iraq war (probably a somewhat over-fluorinated DC, methylphosphonic dichloride) during the 1980s. Iraq additionally used Sarin gas on its own Kurdish population, killing thousands of citizens in the town of Halabja in 1988. Sarin gas was also the weapon used in an attack on the subway in Tokyo in 1995 by the Japanese extremist religious sect Aum Shinrikyo, in which 17 persons were killed and hundreds were injured.

Biological weapons are also capable of mass human destruction. The basic action of a biological weapon involves the use of pathogenic (disease-causing) bacteria, viruses, fungi, or toxins produced by some bacteria. Biological weapons contain particular dangers because they can provoke perilous diseases in people and animals over large geographic areas, as the effectiveness of the weapon multiplies with the spreading of communicable disease. The destructive period can be lengthy with the use of a biological weapon, and it can have latent (incubation) period of action.

What makes biological weapons so dangerous are that the cost to produce such weapons is nominal as compared to the cost to make nuclear weapons. This is why biological weapons are often considered as the terrorist or poor nation's weapon of mass destruction. Also, the production of biological weapons can be easily hidden, as there are no special factories or highly specialized equipment needed for their production. Biological weapons can be deployed silently, through crude crop dusters, the mail, or even bug bombs, therefore allowing for the initial escape of their deployers. Unlike their counterparts (chemical and nuclear weaponry), biological weaponry products are living organisms and do not break down overtime, but in-fact can multiply and increase in numbers.

There is a long list of BW agents that could potentially be used in a war or a terrorist attack. Among those mentioned have been anthrax, cryptosporidiosis, *Yersinia pestis* (plague, the Black Death of the 14th Century), tularemia (rabbit fever), malaria, cholera, typhoid, smallpox, cobra venom, and others. Some authors have also speculated

about the possible terrorist use of new, genetically engineered agents designed to defeat conventional methods of treatment, or to attack specific peoples.

The idea of using biological agents in war is not new. In the 6th century B.C., Solon of Athens used the purgative herb hellebore (skunk cabbage) to poison the water supply during the siege of Krissa. In 1346, plague broke out in the Tartar army during its siege of Kaffa (at present day Feodosiys in the Crimea), after attackers hurled the corpses of those who died over the city walls. The plague epidemic that followed forced the defenders to surrender, and some infected people who left Kaffa may have started the Black Death pandemic that later spread throughout Europe. In 1797, Napoleon attempted to infect the inhabitants of the besieged city of Mantua with swamp fever during his Italian campaign. An attempted biological attack was undertaken in 1915 by the German-American physician Dr. Anton Dilger (in Baltimore) who attempted to infect a reported 3000 head of horses, mules, and cattle destined for the Allied forces in Europe. Nowadays, the specter of annihilation by killer pathogens or toxins has, in some sense, replaced the Cold War nightmare of extermination by massive nuclear attack.

Since 1972, the use of biological weapons is prohibited by the international treaty, as reflected in its formal title, the Convention on the Prohibition of the Development, Production, and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction. As of 2003, the agreement had 144 nation-state signatories.

#### ■ FURTHER READING:

##### BOOKS:

- Cirincione, Joseph, Jon B. Wolfsthal, Miriam Rajkuman, Jessica T. Mathews. *Deadly Arsenals: Tracking Weapons of Mass Destruction*. Washington, DC: Carnegie Endowment for International Peace, 2002.
- Hamzah, Khidr Ald Al-Abbis, and Jeff Stein. *Saddam's Bombmaker: The Terrifying Inside Story of the Iraq Nuclear and Biological Weapons Agenda*. New York: Scribner, 2002.
- Harris, Robert, and Jeremy Paxman. *A Higher Form of Killing: The Secret History of Chemical and Biological Warfare*. New York: Random House, 2002.
- Lavoy, Peter R., Scott D. Sagan, James J. Wirtz. *Planning the Unthinkable: How New Powers Will Use Nuclear, Biological, and Chemical Weapons*. Cornell: Cornell University Press, 2001.
- Rhodes, Richard. *Dark Sun: The Making of the Hydrogen Bomb (Sloan Technology Series)*. Simon & Schuster, 1995.
- Roberts, Brad. *Biological Weapons: Weapons of the Future?* Washington, D.C.: Center for Strategic and International Studies, 1993.
- Sagan, Scott D. and Kenneth N. Waltz. *The Spread of Nuclear Weapons: A Debate Renewed*, Second Edition. W W Norton & Co., 2003.
- Walmer, Max. *An Illustrated Guide to Strategic Weapons*. New York: Prentice Hall Press, 1998.

## PERIODICALS:

- DaSilva, E., "Biological Warfare, Terrorism, and the Biological Toxin Weapons Convention." *Electronic Journal of Biotechnology* 3(1999):1–17.
- Dire, D.J., and T.W. McGovern. "CBRNE—Biological Warfare Agents." *eMedicine Journal*, 4 (2002):1–39.
- Macintrye, A. G., C. G. W. Eitzen, Jr., and R. Gum, et al. "Weapons of Mass Destruction Events with Contaminated Casualties: Effective Planning for Health Care Facilities." *Journal of the American Medical Association* no. 283 (2000): 252–253.
- Munro, N.B., S.S. Talmage, G.D. Griffin, et al. "The Sources, Fate, and Toxicity of Chemical Warfare Agent Degradation Products." *Environmental Health Perspectives* no. 107 (1999): 933–974.
- Nakajima, T., S. Ohta, Y. Fukushima, et al. "Sequelae of Sarin Toxicity at One and Three Years after Exposure in Matsumoto, Japan." *Journal of Epidemiology* no. 9 (1999): 337–343.

## ELECTRONIC:

- How Stuff Works. "How Biological and Chemical Warfare Works." 2002. <<http://www.howstuffworks.com/Biochem-war.htm>>(10 January 2003).
- United States Department of State. "Parties and Signatories of the Biological Weapons Convention." December 11, 2002. <<http://www.state.gov/t/ac/bw/fs/2002/8026.htm>> (February 25, 2003).

## SEE ALSO

- Anthrax, Terrorist Use as a Biological Weapon*  
*Anthrax Vaccine*  
*Anthrax Weaponization*  
*Arms Control, United States Bureau*  
*Biological Warfare*  
*Biological Warfare, Advanced diagnostics*  
*Biological Weapons, Genetic Identification*  
*Bioterrorism, Protective Measures*  
*Chemical Warfare*  
*Manhattan Project*  
*North Korean Nuclear Weapons Programs*  
*Nuclear Detection Devices*  
*Russian Nuclear Materials, Security Issues*  
*Tabun*  
*USAMRIID (United States Army Medical Research Institute of Infectious Diseases)*  
*Vozrozhdeniye Island, Soviet and Russian Biochemical Facility*  
*World War I*  
*World War II*

An atomic bomb exploded over a densely populated city could kill hundreds of thousands of people instantaneously and, as the lethal effects of radiation exposure take hold, causes many more deaths within days or weeks. Chemicals such as Ricin that disrupt nerve function are lethal upon exposure. Agents such as mustard gas can cause life-threatening burns. Chemical weapons can affect a wide geographical area because the chemicals are dispersed in the air.

Biological weapons take longer than nuclear and chemical weapons to cause damage. Because infections can subsequently spread through a population far from the site of contamination, and because the population may not be protected by vaccination or natural immunity to the microorganism responsible for the infection, the eventual death toll from an organized biological attack, however, could reach into the millions. Relevant modern day examples of biological weapons of mass destruction are anthrax (caused by *Bacillus anthracis*), plague (caused by *Yersinia pestis*), and smallpox (caused by the variola virus).

The damage from weapons that are less powerful or toxic can be minimized. For example, buildings can be fortified to withstand assaults from conventional explosives such as grenades. Thus, for such weapons, damage prevention can be the priority rather than detection. However, the damage from a weapon of mass destruction cannot be minimized once the weapon has been unleashed. Rather, the weapons need to be detected before they are used.

## Detection of Chemical and Nuclear Weapons of Mass Destruction

Chemical and nuclear weapons are often delivered to their target in missiles. Sophisticated open-air launch facilities and large pieces of equipment are required for launch, and it is difficult to conceal such facilities from aerial surveillance. Planes, unmanned drones, and even satellites positioned over a region will all reveal the presence of a missile installation. Underground chemical storage facilities can also be revealed by the use of ground penetrating radar.

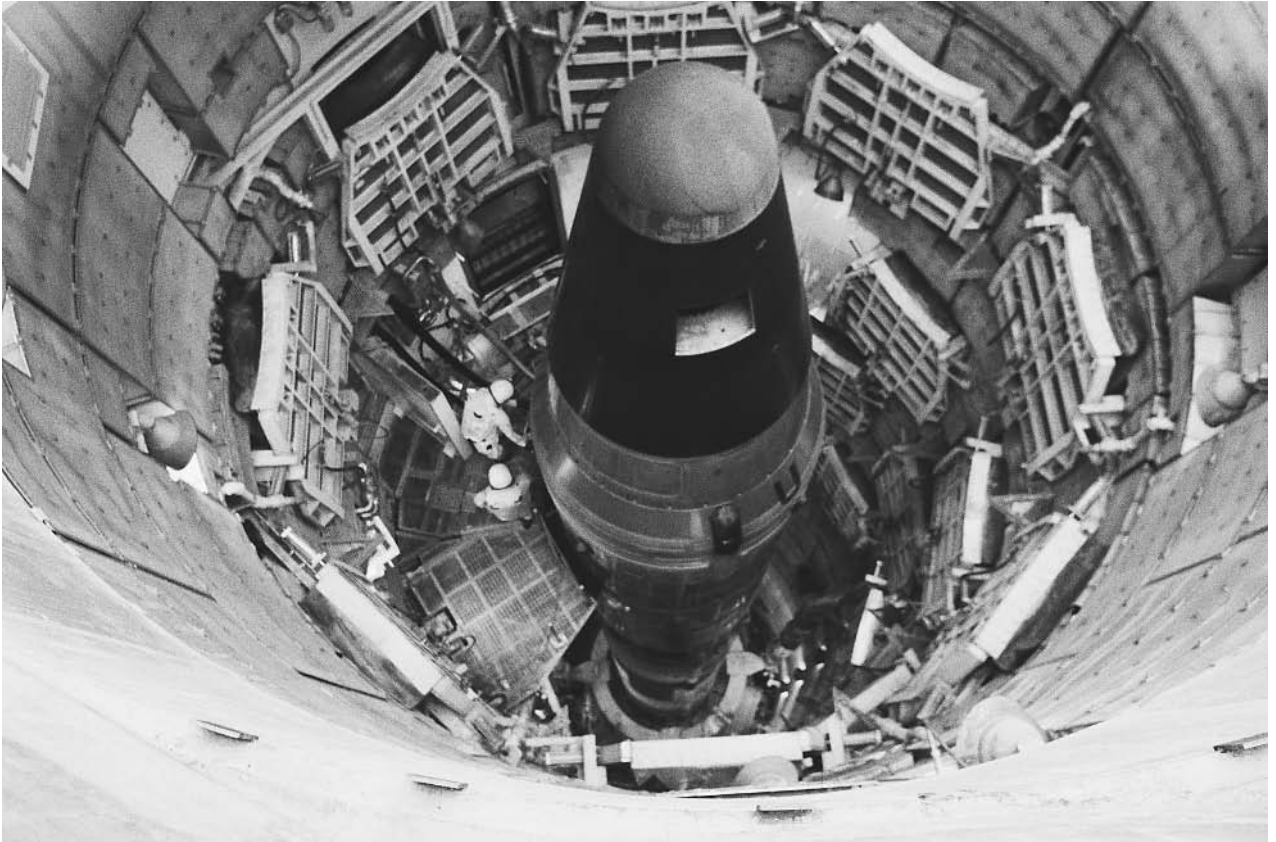
The materials that are commonly used in the construction of chemical and nuclear weapons can be detected. For example, an instrument called the Dual-Use Analyzer uses the phenomenon of eddy current. An electrical current is passed through a sample, and the conductivity of the metal produces a characteristic signal. If another metal is present, such as those used in chemical and nuclear weapons, another signal is produced. The rogue signal can be compared to a databank of signals produced by metals that are typically used in weapons.

**Light or radiation.** The airborne release of chemical weapons can be detected using light. Specifically, the scattering or absorption of a directed beam of laser light, or

## Weapons of Mass Destruction, Detection

■ K. LEE LERNER/BRIAN HOYLE

Weapons of mass destruction are weapons that cause a high loss of life within a short time span. Nuclear, chemical, and biological weapons fit this definition.



Interior of an intercontinental ballistic missile silo. ©STEVE JAY CRISE/CORBIS.

the development of fluorescence when the aerosol cloud contacts laser or ultraviolet light, can detect a chemical cloud at a distance. This sort of detection is not specific. The identity of the compound in the aerosol cloud cannot be determined. But detection can provide some time for preparations (i.e., evacuation gathering in an airtight facility). Specific detection methods, however, are possible. Chemical groups behave in distinctive ways when exposed to different kinds of light or radiation. The measurement of the chemical behavior is called spectroscopy. The machines that perform the analysis are called spectrometers.

In mass spectroscopy, the mass (or molecular weight) of proteins is determined. The molecular weight is an important means of identifying a protein. In turn, the identification of a protein can provide a clue as to what chemical agent is present. Raman spectroscopy relies on the change in the shape and frequency of the wave of light (i.e., the wavelength) as it passes through a sample to identify the chemical groups that cause the wavelength change. In neutron spectroscopy, neutrons interact with the chemical groups of the sample. The patterns of these interactions can be measured and used to identify chemical groups. Neutron spectroscopy is especially adept at detecting plutonium, and thus is useful in the detection of nuclear weapons. Finally, optical spectroscopy relies on

the use of ultraviolet and infrared light. The absorption of the light energy by sample chemical groups, and the giving off of light of a different wavelength by the groups, is used to identify compounds, particularly compounds present in certain explosives.

A Geiger counter is a traditional portable radiation detection device. Here, a tube of gas becomes charged when neutrons pass through the tube. The charged particles are converted to an electrical signal that produces a read-out of the intensity of the radiation.

The U.S. Department of Energy's Argonne National Laboratory has developed a portable device that can detect nuclear weapons. The heart of the device is a small wafer made of gallium arsenide—a material that is similar to silicon—that is coated with boron or lithium. The coated wafer can detect neutrons that are given off by radioactive sources like plutonium<sup>239</sup> and uranium<sup>235</sup>. Another portable sensor detects alloys like zirconium, which are typically used in nuclear weapons. The United Nations (U.N.) weapons inspectors in Iraq utilized this sensing technology during inspections in 2003.

**Sound.** Sandi National Laboratories in Albuquerque New Mexico has developed a portable machine that can detect and identify 18 different chemicals in a vapor within a few

minutes. This enables an on-the-spot detection of chemicals, which is applicable to the battlefield or to the detection of a planted chemical weapon. The compounds that can be detected can be present in chemical, nuclear, and biological weapons.

The basis of the detection is the acoustic wave sensor. A quartz surface can detect an electric signal and convert it to an acoustic signal. The acoustic signal then radiates over the quartz surface as a wave. As the wave moves, it encounters a film of material that has been coated onto the quartz. The chemical nature of the coatings determines what acoustic signal will register. The film slows down the speed of the acoustic wave, which can be used to identify the source of the wave.

The technique of acoustic resonance can reveal whether the interior of a missile is solid or whether it houses a liquid. The distinction is based on the resonance, or vibration, from inside a shell as the shell is vibrated by sound waves. Because different chemicals resonate at different frequencies of sound, the technique can even be used to determine the type of chemical housed in the shell. The device was first used by U.N. inspectors in Iraq in 1997.

**Chemical reactions.** Detection of chemical weapons can be accomplished by several methods. One means is by the use of detection paper. Dyes and pH indicator (an indicator of the concentration of hydrogen or hydronium ions in a solution) are incorporated into a cellulose paper. When a drop of liquid that contains a chemical warfare agent is spotted onto the paper, one of the indicators is dissolved (the particular indicator being dependent on the chemical agent present). The result is a color change. For example, mustard agent dissolves a red dye, and nerve agent dissolves a yellow dye. Other compounds like fat, oil, and fuel can also dissolve the dyes, which produces a false positive reaction. But, with careful use of the paper, the presence of chemical warfare agents can be detected.

Mustard gas can also be detected by sucking air through a tube containing an indicator compound. A reaction between the compounds produces a blue color when the tube is heated.

## Detection of Biological Weapons of Mass Destruction

The identification of proteins by mass spectroscopy can be an efficient and rapid way to identify bacteria. An example is Matrix-Assisted Laser Desorption/Ionization Mass Spectroscopy (MALDI-MS). MALDI-MS can separate and detect different proteins in less than one second. The pattern that is produced is analyzed and the areas of the pattern that are unique to bacteria such as *Bacillus anthracis* (the cause of anthrax) and *Yersinia pestis* (the cause of plague) are identified.

**Genetic technologies.** The genetic detection of biological agents has become exquisitely sensitive. Gene probe sensors can detect and identify bacteria based upon the presence of a stretch of genetic material that is unique to the microorganism. An example is the use of the gene probe technology of the polymerase chain reaction (PCR). PCR detects a pre-determined sequence of genetic material and then produces copies of the target region. Millions of copies can be produced within a hour, allowing the sequence to be detected and studied using other tests (i.e., gel electrophoresis).

When PCR was first introduced, the equipment required dedicated space in a lab. Now, however, the equipment has been miniaturized so that it can fit into a standard briefcase. For example, the Lawrence Livermore Laboratory has developed the Handheld Advanced Nucleic Acid Analyzer (HANAA). The HANAA is about the size of a brick. The genetic probes that are used are designed to detect specific microorganisms. The microbes of interest are *Bacillus anthracis* and *Yersinia pestis*. The unit is being used in the 2003 inspection of Iraqi facilities by U.N. officials, an inspection that is designed to verify Iraq's submitted list of biological weapons, and to reveal any expansion of the nation's biological warfare program since the Gulf War of the mid 1990s.

In contrast to the handheld detector, which operates periodically and under human control, the Autonomous Pathogen Detection System (APDS) is designed to operate continuously and without operator assistance. A fan pulls in air, and any biological material is used for PCR analysis. The APDS, which is about the size of a mailbox, is positioned where round the clock monitoring is critical. The unit can be programmed to sound an alarm when a chemical unique to bacterial spores (including anthrax spores) is present. As well another reaction causes the development of fluorescence. The intensity of the fluorescence is related to the number of spores present.

In 2002, the PCR technology was successfully adapted to allow the detection of the smallpox virus within a few minutes. As of 2003, the rapid test for smallpox is still being refined in the laboratory. However, it will doubtless not be long before the smallpox test is portable enough for use in the field.

Microorganisms can also be rapidly detected using antibodies that have been produced to certain components of the organisms. The binding of the antibody to the corresponding antigen can identify *Bacillus anthracis* in 15 minutes, for example. The same technology can be used with antibodies to other bacteria (e.g., *Clostridium botulinum* and viruses (e.g., smallpox), as well as to chemicals such as ricin.

**Electrophoresis and chromatography.** If a sample is suspected of containing a biological threat, the genetic material (deoxyribonucleic acid; DNA) present in the sample solution can be extracted from the other materials and analyzed. The analysis involves cutting the DNA into a variety

of pieces using enzymes that recognize specific sequences of nucleotides (the building blocks of the DNA). When the pieces of DNA are electrophoresed a series of bands results in the electrophoretic gel. The pattern of the bands is compared to patterns in a database. If an exact match is found, then the identify of the microorganism is established.

The various types of chromatography all distinguish different chemical groups from one another by the varying behaviors of the groups in certain environments. For example, one chemical group may move more slowly through a certain liquid than another chemical group. Thus, the two groups can be separated from one another. Furthermore, the pattern of their movements provides a fingerprint to identify the chemical natures of the compounds.

Microorganisms can be detected by a technique called gas liquid chromatography. The method detects fatty acids, which are a portion of the lipid molecules that make up the membrane(s) that surround microorganisms. This type of detection still requires a bulky machine and the use of specialized personnel. Nonetheless, if the need for detection is on the order of days rather than minutes, then fatty acid analysis is a useful and accurate technique.

**Filters.** Microorganisms like bacteria and fungi that are floating in the air can be detected by sucking the air through a filter. The filter traps the microorganisms. The filter is then placed in contact with a food source that encourages the growth and division of the bacterial or fungal cells. Within about 24 to 48 hours the microorganisms have grown and reproduced enough to form a visible clump of cells called a colony. This technology is also portable.

## Detection of Weapons of Mass Destruction in Iraq

In November 2002, a team of 220 inspectors—with 50 more to join within weeks—began examining a variety of sites throughout Iraq for the presence of chemical, nuclear, and biological weapons of mass destruction. During the 1990s, Iraq acknowledged having such weapons and weapons development programs. However, Iraqi officials reported that these activities were ended.

The weapons inspection occurring in Iraq in 2003 utilized a variety of weapons detections technologies. Surveillance planes such as the unmanned Predator drone are equipped with high-resolution cameras and provided aerial views of the selected terrain. Detailed images from surveillance satellites placed in orbit over a selected part of the globe provided details of construction projects or the presence of equipment that might be used for weapons. Other cameras were utilized on the ground. Digital cameras can be left in place after an inspection is complete, to provide a longer-term monitoring of the site. Ground penetrating radar positioned on helicopters or

unmanned drones was used to seek buried caches of missile components and bunkers that could house weapons. Finally, the portable sensors that have been described were used.

### ■ FURTHER READING:

#### BOOKS:

Butler, Richard. *The Greatest Threat: Iraq, Weapons of Mass Destruction, and the Crisis of Global Security*. New York: Public Affairs, 2001.

Cirincione, Joseph, Jon B. Wolfsthal, and Jessica T. Mathews. *Deadly Assaults: Tracking Weapons of Mass Destruction*. Washington, D.C.: Carnegie Endowment for International Peace, 2002.

#### PERIODICALS:

LeDuc, J.W., I. Damar, J.M. Meegan, et al. "Smallpox Research Activities: U.S. Interagency Collaboration 2001." *Emerging and Infectious Diseases* 8 (2002): 743–45.

Reeves, A. "Tracing Biothreats with Molecular Signatures." *Los Alamos National Laboratory Research Quarterly* Fall 2002: 15–17.

#### ELECTRONIC:

Lawrence Livermore National Laboratory. "Reducing the Threat of Biological Weapons." Chemical/Biological Nonproliferation Program. June 1998. <<http://www.llnl.gov/str/Milan.html>>(7 January 2003).

#### SEE ALSO

*Anthrax Weaponization*  
*Ballistic Missiles*  
*Biological Warfare*  
*Biosensor Technologies*  
*Chemical Warfare*  
*Pathogens*  
*Spores*

## Weather Alteration.

SEE *Meteorology and Weather Alteration*.

---

## Windtalkers

---

### ■ ADRIENNE WILMOTH LERNER

Windtalkers was the code name given to the Navajo Indian code talkers employed by United States military intelligence during World War II. Agents developed several encryption methods and code systems during the war, but a code based on the ancient Navajo language was one of





A two-man team of Navajo code talkers attached to a marine regiment in the Pacific relay orders over the field radio using their native Navajo language, a particularly effective code used during World War II. ©CORBIS.

the most successful codes ever used. It remained unbroken throughout the course of the war.

The Navajo code was not the first attempt to use Native American languages to disguise military communications. During World War I, the military adopted the Choctaw language as a code and employed Choctaw code talkers. Indigenous languages attracted code experts because most had no systems of writing and were spoken by a small number of people. The first attempts to utilize Indian languages as code simply involved using the spoken language and translating the messages into English. The language itself functioned as the code, and no additional encryption methods were employed to encipher communications.

In 1939, as World War II began in Europe, the American Army Signal Corps and Naval Intelligence renewed their interest in developing sophisticated enciphering methods. Both Allied and Axis forces relied on new cipher machines and complex mathematical encryption tables for encoding messages. Intelligence service cryptologists broke many of these, such as the German Enigma machine. Codebooks were risky, and too easily recovered by enemy forces. These developments forced cryptologists to change codes often, requiring tedious work. Code experts sought a code that would be simple to use, functional, and secure for the duration of the war.

World War I veteran and civil engineer Philip Johnston proposed the use of a Native American language in conjunction with a letter-symbol replacement encryption system. The son of a missionary, Johnston was raised on a Navajo reservation and spoke the Navajo language fluently. He thought the indigenous language a perfect candidate to use as the basis for a code, largely because of its obscurity. The language had never developed a system of writing, but possessed a great flexibility in its descriptive word combinations. In addition, Navajo men served in cooperation with American forces in World War I, despite tensions during the era between the American government and Indian nations. Military intelligence accepted Johnston's proposal. The project was granted to the Marine Corps for development and supervision. In 1941, the first twenty-nine Navajo code talkers were recruited into service as Marine Corps Radio Operators.

The first twenty-nine recruits worked with Johnston and Marine Corps officials to develop the Navajo language-based code eventually used in the Pacific theater of war. The initial draft of the code consisted of 211 key words and military terms. For the names of places and people, the code used Navajo words to spell out proper nouns by taking the first letter of the word's English equivalent. Because several words could be used to represent one letter in the Latin alphabet, the code was flexible for knowledgeable users, but enigmatic to code breakers. The Navajo code talkers also had to invent Navajo words to represent frequently used military terms. For example, because the Navajo had no word for submarine, they used *besh-lo*, literally meaning "iron fish." Eventually, most radio transmissions were encoded using the word-for-letter replacement system. In 1943, Navajo code talker units experimented with overlaying the Navajo code with a mathematical encryption system. While this method was used with great success to guard classified and highly secret wire transmissions, and could be used in conjunction with cipher machines, the process was too tedious for rapid, battlefield communication.

After months of developing a functional code, the original Navajo code talkers reported for basic training at Camp Elliot, California, in May 1942. Three months later, on August 7, twenty-seven code talkers, designated the 382nd Platoon, departed for their first assignment among the invasion forces at Guadalcanal. The code was used during the battle with great success. Commanding officers complained that other ciphered messages took two hours to send and decode. The Navajo code efficiently transmitted communications in mere minutes. After the battle, the Marine Corps established a radio and wire transmission station for the Pacific fleet. Within weeks, use of the Navajo code increased, eventually encompassing a quarter of all communications sent from the station. The Navajo code also became the cryptological method of choice for urgent communications on the front lines. Realizing the need for more personnel skilled in the Navajo language and trained for code talking, the military founded the Navajo Code Talkers Program at Camp Pendleton,

California. There, Navajo recruits memorized the complex code, and completed specialized equipment training.

Over 540 Navajo served in the Marines during World War II, nearly 300 served in the field as code and communication experts. Navajo code talkers operated in all six Marine divisions, and served in every major Pacific battle between 1942 and 1945. At the battle of Iwo Jima, a small unit of six Navajo code talkers, under the command of 5th Marine Division signal officer, Major Howard Connor, transmitted and received nearly 1,000 messages in 48 hours. The unit garnered a reputation for working ceaselessly, and without error. The security of the Navajo code, in conjunction with the work of American cryptologists who broke several important Japanese codes, gave the Allied forces a decisive intelligence advantage in the Pacific.

Johnston's code was as functional and unbreakable as he originally asserted. The code not only remained uncracked throughout the course of World War II, but also was used in the Korean and Vietnam Wars with similar success. Other indigenous languages, such as those of the Choctaw, Chippewa, Creek, Sioux, and other tribes, were explored as possible sources for military codes both before and after World War II. However, none were more widely used or accomplished than the Navajo code. The code was eventually retired from use and declassified in 1968.

On July 26, 2001, Congress awarded the Congressional Gold Medal to the original twenty-nine Navajo code talkers who aided in the development in the code. The remaining veteran Windtalkers were awarded the Congressional Silver Medal.

#### ■ FURTHER READING:

##### BOOKS:

Bixler, Margaret T. *Winds of Freedom: The Story of the Navajo Code Talkers of World War II*. Darien, CT: Two Bytes Publishing Company, 1992.

Kawano, Kenji. *Warriors: Navajo Code Talkers*. Flagstaff, AZ: Northland, 1990.

##### PERIODICALS:

Watson, Bruce. "Navajo Code Talkers: A Few Good Men." *Smithsonian*. 24, no.5, August 1993.

##### SEE ALSO

*Codes and Ciphers*  
*Codes, Fast and Scalable Scientific Computation*  
*World War II, United States Breaking of Japanese Naval Codes*

## Wire Tap.

SEE *Bugs (microphones) and Bug Detectors*.

## World Health Organization (WHO)

■ BRIAN D. HOYLE

The World Health Organization (WHO) is the principal international organization managing public health-related issues on a global scale. Headquartered in Geneva, the WHO is comprised of 191 member states (e.g., countries) from around the globe. The organization contributes to international public health in areas including disease prevention and control, promotion of good health, addressing disease outbreaks, initiatives to eliminate diseases (e.g., vaccination programs), and development of treatment and prevention standards.

In 2003, WHO began to coordinate global efforts to monitor the outbreak of the virus responsible for Severe Acute Respiratory Syndrome (SARS). WHO officials also directed aspects of research efforts to identify the specific virus responsible. In addition, WHO officials issued specific recommendations with regard to isolation and quarantine policy and issued alerts for travelers.

Just after the end of World War I, the League of Nations was created to promote peace and security in the aftermath of the war. One of the mandates of the League of Nations was the prevention and control of disease around the world. The Health Organization of the League of Nations was established for this purpose, and was headquartered in Geneva. In 1945, the United Nations Conference on International Organization in San Francisco approved a motion put forth by Brazil and China to establish a new and independent international organization devoted to public health. The proposed organization was meant to unite the number of disparate health organizations that had been established in various countries around the world. The following year this resolution was formally enacted at the International Health Conference in New York, and the Constitution of the World Health organization was approved.

In its constitution, WHO defines health as not merely the absence of disease. A definition that subsequently paved the way for WHO's involvement in the preventative aspects of disease.

From its inception, WHO has been involved in public health campaigns that focused on the improvement of sanitary conditions. In 1951, the Fourth World Health Assembly adopted a WHO document proposing new international sanitary regulations. Additionally, WHO mounted extensive vaccination campaigns against a number of diseases of microbial origin, including poliomyelitis, measles, diphtheria, whooping cough, tetanus, tuberculosis, and smallpox. The latter campaign has been extremely successful, with the last known natural case of smallpox having occurred in 1977. The elimination of

poliomyelitis is expected by the end of the first decade of the twenty-first century.

Another noteworthy initiative of WHO has been the Global Program on AIDS, which was launched in 1987. The participation of WHO and agencies such as the Centers for Disease Control and Prevention is necessary to adequately address AIDS, because the disease is prevalent in under-developed countries where access to medical care and health promotion is limited.

Today, WHO is structured as eight divisions addressing communicable diseases, noncommunicable diseases and mental health, family and community health, sustainable development and health environments, health technology and pharmaceuticals, and policy development. These divisions support the four pillars of WHO: worldwide guidance in health, worldwide development of improved standards of health, cooperation with governments in strengthening national health programs, and development of improved health technologies, information, and standards.

#### ■ FURTHER READING:

##### ELECTRONIC:

World Health Organization. May, 2003. <<http://www.who.int/en/>> (May 10, 2003).

##### SEE ALSO

*CDC (United States Centers for Disease Control and Prevention)*  
*Public Health Service (PHS), United States*

---

## World Trade Center, 1993 Terrorist Attack

---

#### ■ JUDSON KNIGHT

The World Trade Center (WTC) bombing of 1993 has long since been overshadowed by the attack that brought the twin towers down on September 11, 2001. Yet, at the time it occurred, the attack loomed as large on the American landscape as the towers themselves once did on the Manhattan skyline. The attack killed six people and injured more than a thousand, the first casualties from foreign terrorists on U.S. soil. American authorities identified at least eight perpetrators, but questions remain as to the ultimate cause of the attack.

**The attack and its aftermath.** At 12:18 p.m. on Friday, February 26, 1993, an explosion rocked the second level of the parking basement beneath Trade Tower One. The explosive material, as investigators would later determine, was somewhere between 1,200 and 1,500 pounds

(544–680 kg) of urea nitrate, a homemade fertilizer-based explosive.

The blast ripped open a crater 150 feet (46 m) in diameter and five floors deep, rupturing sewer and water mains and cutting off electricity. Over the hours that followed, more than 50,000 people were evacuated from the Trade Center complex. A stunned nation soon grasped a fact larger than the incident itself: foreign-sponsored terrorism—which had long plagued Western Europe and parts of the Middle East, Africa, and Asia—had come to the United States.

**Investigation and cleanup begins.** The first analysis team to arrive came from the Federal Bureau of Investigation (FBI), who soon brought in two examiners from the FBI Laboratory Explosives Unit. Over the week that followed, a team of more than 300 law-enforcement officers from various agencies throughout the country would sift through some 2,500 cubic yards (1,911 cubic meters) of debris weighing more than 6,800 tons (6,909 tonnes).

At the same time that this forensic investigation began, government authorities rushed to protect against physical, chemical, and biological hazards associated with the blast. The explosion had exposed raw sewage, asbestos, mineral wool, acid, and fumes from automobiles. Meanwhile, small electrical fires burned, and pieces of concrete and sharp metal hung threateningly from distended beams.

On Saturday, authorities installed seismographic equipment, cleared the area, and conducted a test run of an empty subway train. The results showed that with a few adjustments, the area could be rendered safe for the operation of the Port Authority Transportation system (PATH) on Monday, thus preventing a virtual shutdown of lower Manhattan. The Environmental Protection Agency and the Occupational Safety and Health Administration began taking steps to clean up biological and chemical debris.

**Tracking the killers.** Meanwhile, the forensic investigation expanded, with two chemists each from the FBI, ATF (Bureau of Alcohol, Tobacco, and Firearms), and New York Police Department collecting and studying residue from the blast area. In the course of this work, investigators found a key piece of evidence: a 300-pound (136-kg) fragment of a vehicle that, based on the damage it had sustained, must have been at the very epicenter of the blast. Sewage contamination had rendered it unusable for residue analysis, but it bore something much better: a vehicle identification number (VIN).

This was not to be the first fortunate break for investigators. Authorities traced the vehicle to a Ryder truck rental facility in Jersey City, New Jersey, from which it had been reported stolen. On Monday, while FBI special agents were at the Jersey City facility to speak with personnel there, the Ryder clerk received a call from a man identified as Mohamed Saleme. The latter demanded the return of



FBI agents view the damage caused by the 1993 terrorist bombing of the parking garage at the World Trade Center towers in New York. ©REUTERS NEWMEDIA INC./CORBIS.

his \$400 deposit for the van in question, and the Ryder clerk arranged for him to return and collect the deposit on March 4, 1993. When Salemeah arrived, he was arrested.

A search of Salemeah's belongings led investigators to Nidal Ayad, a chemist working for the Allied Signal Corporation in New Jersey. Toll records and receipts helped lead to a safe house in Jersey City, New Jersey, where authorities found traces of nitroglycerine and urea nitrate. They also uncovered evidence that Salemeah and Ayad had obtained three tanks of compressed hydrogen gas, and in the course of searching a storage room rented by Salemeah, investigators found large caches of urea, sulfuric acid, and other chemicals used in making a bomb. On March 3, the *New York Times* received a letter claiming responsibility for the bombing, and subsequent investigation of DNA samples matched Ayad with the saliva on the envelope flap.

**Conviction—and continuing questions.** The trail of investigation would eventually lead to Ramzi Yousef, who authorities believe was in the van that delivered the explosives to the WTC. With him was Eyad Ismoil. Also implicated in the bombing, along with Salemeah and Ayad, were

Ahmad Ajaj, Mahmoud Abouhalima, and Abdul Rahman Yasin. On March 4, 1994, a jury found Salemeah, Ajaj, Abouhalima, and Ayad guilty on 38 counts, including murder and conspiracy, and the judge handed down multiple life sentences.

Yousef fled the country, and engaged in other terror plots before he was captured and brought to the United States from Pakistan in February 1995. He was sentenced to life plus 240 years. As of 2003, Yasin had not been captured, and was believed to be in Iraq. In October 1995, Sheikh Omar Abdel Rahman, a blind Egyptian cleric who taught at mosques in Brooklyn and New Jersey, was sentenced to life imprisonment for masterminding the attack. But some observers wonder whether the roots of the 1993 WTC attack run much deeper.

The fact that Yousef is the nephew of Khalid Sheikh Mohammed, a top figure in al-Qaeda, suggests a strong connection between the 1993 conspirators and the group who ultimately brought down the towers eight years later. After the September 2001, attack, it was the opinion of many investigators and analysts inside President George W. Bush's administration, that the perpetrators of that attack had a state sponsor—Iraq. A number of details,

including the fact that Yousef was traveling on an Iraqi passport, as well as the date of the 1993 attack—the second anniversary of the U.S. liberation of Kuwait in the Persian Gulf War—furthered suspicions of Iraqi involvement in the 1993 incident. Mohammed was later involved in masterminding the terrorist attacks on the World Trade Center in 2001, and was arrested in Rawalpindi, Pakistan on March 1, 2003.

#### ■ FURTHER READING:

##### BOOKS:

Dwyer, Jim. *Two Seconds Under the World: Terror Comes to America*. New York: Crown Publishers, 1994.

Gillespie, Angus K. *Twin Towers: The Life of New York City's World Trade Center*. New Brunswick, NJ: Rutgers University Press, 1999.

Juergensmeyer, Mark. *Terror in the Mind of God: The Global Rise of Religious Violence*. Berkeley: University of California Press, 2000.

Mylroie, Laurie. *Study of Revenge: The First World Trade Center Attack and Saddam Hussein's War against America*. Washington, D.C.: AEI Press, 2001.

Reeve, Simon. *The New Jackals: Ramzi Yousef, Osama bin Laden, and the Future of Terrorism*. Boston: Northeastern University Press, 1999.

##### ELECTRONIC:

Hirschhorn, Phil. Top Terrorist Convictions Upheld. Cable News Network. <<http://www.cnn.com/2003/LAW/04/04/terrorism.yousef/>> (April 7, 2003).

##### SEE ALSO

*Bomb Damage, Forensic Assessment Clinton Administration (1993–2001), United States National Security Policy*  
*United States, Counter-terrorism Policy*  
*Terrorist and Para-State Organizations*  
*World Trade Center, 2001 Terrorist Attack*

---

## World Trade Center, 2001 Terrorist Attack

---

#### ■ JUDSON KNIGHT

At 8:46 a.m. on September 11, 2001, American Airlines Flight 11, hijacked from Boston's Logan Airport with 92 people on board, crashed into the upper floors of the World Trade Center north tower in lower Manhattan, New York. Seventeen minutes later, United Airlines Flight 175, also hijacked from Logan and with 65 people on board, crashed into the south tower. By this time, virtually the entire nation had tuned in to witness the after-effects on television of what at first seemed a terrible accident, but

was quickly revealed as a terrorist attack. Over the course of the next 85 minutes, the south tower collapsed, followed by the collapse of the north tower. The incident, in which nearly 3,000 people died, ranks as by far the worst case of mass murder in U.S. history, the worst building disaster in human history, and the largest terrorist incident in the history of the western world.

### The Towers and their Environment

Designed by architect Minoru Yamasaki—who, ironically, had a fear of heights—and engineered by Leslie Robertson and John Skilling, the 110-story towers soared 1,360 feet (415 m) above an open plaza, which made them the world's tallest buildings at the time of their completion in 1973. Whereas the Empire State Building and other older skyscrapers drew support from an interior grid of steel girders, support for the trade towers came from the exterior and the inner core. Horizontal floor trusses joined the perimeter support structure to the central area, which the engineers envisioned as a great “tube” running through the building and containing not only its support structure, but also its utilities such as elevators. This design had two advantages; it made the buildings extremely stable—not prone to swaying in high winds as the Empire State did—and it left much of the interior available as rentable space.

To support such a structure required a strong foundation, and in this regard, the location in lower Manhattan was not a promising one. Bedrock lay between 55 and 80 feet (17–24 m) below street level, and to get to it, construction crews had to deal with another engineering challenge: flooding from the nearby Hudson River. In order to dig without flooding the site, they dug narrow trenches to the bedrock, and as they went, they pumped in a slurry of water and bentonite, a type of clay that expanded to prevent groundwater from flowing in. The slurry trench method made it possible to build a watertight framework for the excavation of the foundation structure, nicknamed “the bathtub.”

Excavation began in 1966, and yielded such a quantity of fill that it was used to reclaim 28 acres (11.3 hectares) from the Hudson to form Battery Park City. In addition to supports, in the area underneath the buildings would be seven stories of parking decks, stores, and subway lines. The erection of the buildings themselves, which took more than five years, was a massive feat of both construction and logistics, involving 200,000 tons (181,437) of steel, each major piece of which was marked with an identification number. Over the years of building, many businesses moved in long before the towers were officially completed.

**28 years in the towers' lives.** On April 4, 1973, the World Trade Center officially opened for business. Though the towers were by far the most notable aspect of the project, they were just two of seven buildings in the entire complex. Built at a cost of \$1 billion, the towers functioned as

virtual cities unto themselves, with some 500 businesses, including banks and their offices, law firms, brokerage houses, television stations, charitable organizations, airlines, and government offices. Supporting these functions and the 50,000 employees who filled them were numerous restaurants—most notable of which was “Windows on the World” at the top of the North Tower—as well as other services, including nine chapels of different faiths.

By the 1980s, New Yorkers had become accustomed to the trade towers, which punctuated the skyline as the ultimate symbol of American commerce. Then, in February 1993, just months before the towers turned 20, the towers became the target for a bombing by Islamist terrorists operating a van filled with explosives. In this, the first terrorist attack, six people were killed, but the structural integrity of the towers themselves was not threatened.

## September 11 and Its Aftermath

Because of the 1993 attack, many Americans who witnessed the events of September 11, 2001, quickly realized that the buildings had once again become the target for terrorists. When Flight 11 crashed into the North Tower of the World Trade Center at 8:46 a.m., smoke and flames began to gush from the upper stories, and workers began to evacuate the lower floors. Some, however, chose to remain at their desks. For workers on the floors above the impact area, there was no choice but to remain in place.

For 17 minutes, it was possible to assume that what had happened to the North Tower was an accident; then, Flight 175 smashed into the South Tower. Once again, smoke and flames erupted from the heights of the building, and tenants down below began a slow, but steady evacuation while others—many with no choice—stayed where they were.

By 9:59 a.m., millions of Americans had turned on their television sets to watch live reports from the site. Thus, there was a vast audience to experience what happened next, an event that would be etched upon the consciousness of an entire nation. With little warning, the South Tower, succumbing to the stress caused by the fire, began to crash from the top down, creating a vast cloud of dust and ash above and filling the streets below with noise and heat and terror.

By 10:28 a.m., the North Tower began to implode, once again crashing downward from the top, and the area around what had once been the World Trade Center became smoke, ash, and dust. The other five buildings in the former World Trade Center complex, including the Marriott Hotel, the Commodities Exchange, Dean Witter, the U.S. Customs House, and 7 World Trade Center, were destroyed as well. The last of these caught fire, and collapsed that night.

**Rescue, cleanup, and the death toll.** In the next days and weeks, some 1,500 firemen, search and rescue workers,

ironworkers, engineers, heavy equipment operators, and others labored at the site where the towers had stood, a place now known variously as “Ground Zero” or “the Hole.” In the shock and horror that followed the attacks, among the few bright spots were the many tales of heroism told by people who owed their lives to police, fire, and medical personnel.

That heroism continued in the weeks of the cleanup, as rescue workers sifted through piles of wreckage. The purpose of their job was manifold. Not only were they cleaning the site, but they were looking for evidence, and—most poignantly—for any signs of the dead.

At first, rescuers had hoped to find survivors trapped under the rubble and trauma centers at local hospitals braced to treat mass casualties, but those hopes faded quickly, and the cleanup work involved sifting through materials that included physical traces of the building’s former inhabitants. Not only was the cleanup work grisly, it was also dangerous: rather than working on solid ground, the rescuers had to set up their cranes and other equipment on top of debris piled several hundred feet above the buildings’ foundations.

The numbers of the dead would emerge slowly, and had yet to be fully authenticated even two years later. Although the dead numbered 2801, it was estimated that at the early morning hour, almost 7000 of the 50,000 people who worked in the buildings were in their offices at the time of the attacks. Although the span of time between the attacks and the collapse of the buildings was little more than an hour, it had been enough for those who were able to do so to evacuate via stairwells.

**Structural explanations.** In late 2001, a team of investigators that included representatives of the American Society of Civil Engineers and the Federal Emergency Management Agency (FEMA) commenced a study on the structural collapse of the towers, the details of which they made public in April 2002. In August 2002, the National Institute of Standards and Technology (NIST) began its own study, scheduled to last two years.

The first team concluded that it was not the impact, but the heat from the burning jet fuel, that heated the temperature of the buildings’ steel support structures up to 800°C (1472°F), causing them to buckle and the floors to collapse downward. (Both jets were bound for Los Angeles and had almost a full complement of fuel on board.) On the other hand, the impact did have the effect of knocking out support columns in the building’s interior, which may have weakened the structure. The initial crash neutralized sprinkler systems, allowing spread of the fire, which was fed by caches of paper and other flammable materials in offices.

Almost all sources, including government officials, architects, and engineers, agreed on key elements of the building damage. First, it would have been virtually impossible to prevent the destruction of the buildings by

aircraft used in the way they were on September 11 as guided missiles. Second, the structural integrity of the buildings that allowed the towers to stand for over an hour after the impacts enabled thousands of people to evacuate. Finally, it was evident that the era of the extremely tall skyscraper was in question. Due to high costs, the construction of very tall buildings had been on the decline in the United States for many years, and the events of 9/11 sealed the fate of some mega-skyscraper projects.

**The perpetrators.** Federal authorities, using financial records and other materials, had long since identified the al-Qaeda terror network as the perpetrators of the attack. Al-Qaeda was not a new name: it and its leader, Osama bin Laden, had been linked with the August 1998 bombings at U.S. embassies in Africa, and with the bombing of the USS *Cole* in Yemen in 2000.

Al-Qaeda had strong links to the Taliban regime in Afghanistan, which gave them asylum. Officials in the administration of President George W. Bush, as well as some observers outside the administration, also held that there were substantive links between al-Qaeda, the terrorists who carried out the 1993 bombing, and the government of Iraq. (In fact, Ramzi Yousef, one of the ring leaders in 1993, was nephew to Khalid Sheikh Mohammed, a top al-Qaeda operative, and considerable evidence—including Yousef's Iraqi passport—linked them to Iraq.) The U.S. military actions against Afghanistan in 2001–2002, and Iraq in 2003, were a response to the 2001 terrorist attacks, whose most potent images revolved around the collapse of the World Trade Center towers.

#### ■ FURTHER READING:

##### BOOKS:

- Halberstam, David. *New York September 11*. New York: PowerHouse Books, 2001.
- Hoge, James F., and Gideon Rose. *How Did This Happen?: Terrorism and the New War*. New York: PublicAffairs, 2001.
- One Nation: America Remembers September 11, 2001*. Boston: Little, Brown, 2001.
- Smith, Dennis. *Report from Ground Zero: The Story of the Rescue Efforts at the World Trade Center*. New York: Viking, 2002.

##### ELECTRONIC:

- Day One—The Attack. Los Angeles Times. <<http://www.latimes.com/news/nationworld/nation/la-dayone-graphics.story>> (April 22, 2003).
- September 11, 2001. How Stuff Works. <<http://www.howstuffworks.com/sept-eleven3.htm>> (April 22, 2003).
- September 11 Archive. <<http://september11.archive.org/>> (April 22, 2003).

##### SEE ALSO

*Enduring Freedom, Operation*

*FEMA (United States Federal Emergency Management Agency)*  
*Iraqi Freedom, Operation (2003 War against Iraq)*  
*Kenya, Bombing of United States Embassy*  
*NIST (United States National Institute of Standards and Technology)*  
*Patriot Act, United States*  
*Persian Gulf War*  
*September 11 Terrorist Attacks on the United States*  
*Terrorist and Para-State Organizations*  
*United States, Counter-terrorism Policy*  
*USS Cole,*  
*World Trade Center, 1993 Terrorist Attack*

## World War I

■ ADRIENNE WILMOTH LERNER

World War I, which spanned a four-year period between 1914 and 1918, erupted as a result of the complicated European alliance system. The assassination of Austrian Archduke Ferdinand, and his wife, Sophie, by Serbian nationalists sparked pan-European conflict when Russia, backed by France, declared their intent to defend Serbia, should Austria declare war. The Austrian government, with its ally Germany, declared war on Serbia three days later. British forces joined the French and Russians, but the United States, home to large immigrant populations of all of the fighting nations, resolved to remain out of the conflict.

The United States declared its neutrality, but the nation harbored Allied sympathies. United States manufacture and trafficking of munitions and supplies to aid British and French forces angered Germany and Austria. The German Navy attacked American ships, potentially loaded with contraband, in the Atlantic, and sent intelligence agents to conduct sabotage operations within the United States. In 1917, German hostility prompted the United States to enter the conflict in Europe.

The war ended in 1918, followed by the formal surrender of German and Austrian forces with the signing of the Treaty of Versailles. However, World War I forever changed modern warfare, introducing the concepts of total warfare and weapons of mass destruction.

**National intelligence communities.** At the outbreak of the war, many nations had weak or fledgling national intelligence communities. The French government and military both maintained trained intelligence forces, but no central agency processed intelligence information, or facilitated the distribution of critical intelligence information. Russia had special agents of the Czar, and secret police forces, but its foreign intelligence infrastructure was almost nonexistent.



Members of the first contingent of New Yorkers drafted into the United States Army are shown lined up in front of their barracks at Camp Upton, Long Island, New York, as America enters World War I in 1917. AP/WIDE WORLD PHOTOS.

The United States developed stronger domestic intelligence and investigative services in the decade before World War I. However, the country's lingering isolationism and neutral posture in the war hampered the development of a foreign intelligence corps until the United States entered the war in 1917.

Britain had a well-developed military intelligence system, coordinated through the Office of Military Intelligence. British intelligence forces engaged in a range of specialized intelligence activities, from wiretapping to human espionage. The vast expanse of British colonial holdings across the globe provided numerous outposts for intelligence operations, and facilitated espionage. British forces were among the first to employ a unit of agents devoted to the practice of industrial espionage, conducting wartime surveillance of German weapons manufacturing.

Of all the warring nations in 1914, Germany possessed the most developed, sophisticated, and extensive intelligence community. The civilian German intelligence service, the *Abwehr*, employed a comprehensive network of spies and informants across Europe, North Africa, the Middle East, and in the United States. German intelligence successfully employed wire taps, infiltrating many foreign government offices before the outbreak of the war.

World War I forced most national intelligence services to rapidly modernize, revising espionage and intelligence tradecraft to fit changing battlefield tactics and technological advances. The experience of the war formed the first modern intelligence services, serving as forerunners of the intelligence communities in France, Britain, Germany, and the United States today.

**Sabotage.** German intelligence trained special agents, most of whom used professional or diplomatic covers in the United States, to conduct acts of sabotage against United States industries that aided the British, French, and Russian allied forces in the war. International rules of engagement limited the ways in which Germany and Austria-Hungary could provoke or attack the declaredly neutral United States. German high command desired to cripple United States aid capabilities, but not provoke the nation to enter the conflict. German undercover agents attacked railroads, warehouses, shipyards, and military installations in 1914 and 1915. Agents attempted to make these attacks appear as accidents, but United States authorities caught several potential saboteurs before they destroyed property, unmasking the German plot. Anti-spy hysteria fueled



public fear and anger regarding the acts of German saboteurs.

German and Austrian agents carried out more than 50 acts of sabotage against United States targets on American soil during the course of the war. Most of the attacks occurred in New York City and the region surrounding New York harbor. The most famous and devastating attack, the sabotage of Black Tom Pier, shook buildings and broke windows across New York City and suburban New Jersey. The July 29, 1916, explosion destroyed several ships and waterfront ammunition storage facilities. The attack decimated Black Tom Pier, the staging area for most shipments bound for the Western Front in Europe.

German sabotage attacks in the United States, while successful, only managed to strike at a handful of military and shipping targets. The United States government continued to aid British and French forces in Europe, but the attacks inflamed pro-war sentiment.

**Communications and cryptology.** Advancements in communications and transportation necessitated the development of new means of protecting messages from falling into enemy hands. Though an ancient art, cryptology evolved to fit modern communication needs during World War I. The telegraph aided long-distance communication between command and the battlefield, but lines were vulnerable to enemy tapping. All parties in the conflict relied heavily on codes to protect sensitive information. Cryptology, the science of codes, advanced considerably during the first year of the war. Complex mathematical codes took the place of any older, simple replacement and substitution codes. Breaking the new codes required the employment of cryptology experts trained in mathematics, logic, or modern languages. As the operation of codes became more involved, the necessity for centralized cryptanalysis bureaus became evident. These bureaus employed code breakers, translators, counterintelligence personnel, and agents of espionage.

The most common codes used during the war continued to be substitution codes. However, most important messages were encrypted. Encryption further disguised messages by applying a second, mathematical code to the encoded message. Encryption and coding both required the use of codebooks to send and receive messages. These books proved to be a security liability for the military. During the course of the war, four separate German diplomatic and military corps code books fell into the hands of British intelligence, compromising the security of German communications for the rest of the war.

Both the Germans and the British broke each other's World War I codes with varying success. The German *Abwehr* broke several British diplomatic and Naval codes, permitting German U-boats to track and sink ships containing munitions. British cryptanalysis forces at Room 40, the military intelligence code-breaking bureau, successfully deciphered numerous German codes, thanks in large part to the capture of German codebooks. In 1917,

British intelligence intercepted a diplomatic message between Berlin and Mexico City, relayed through Washington. The message, known as the Zimmerman Telegram, noted German plans to conduct unrestricted warfare against American ships in the Atlantic, and offered to return parts of Texas and California to Mexico in exchange for their assistance. Discovery of the Zimmerman Telegram prompted the United States to enter World War I.

Cryptology, once the exclusive tool of diplomats and military leaders, became the responsibility of the modern intelligence community. After World War I, many nations dissolved their wartime intelligence services, but kept their cryptanalysis bureaus, a nod to the growing importance of communications intelligence and espionage.

**Trench warfare and the evolution of strategic espionage tradecraft.** The advent of trench warfare necessitated the development of new surveillance and espionage techniques to locate enemy positions and gauge troop strength. Crossing "no man's land," the area between trench fronts, was dangerous, and using human scouts proved costly to both sides in the early months of the war. Military intelligence officers instead relied on networks of local citizens for information on enemy advances and supply lines. Finding sympathetic locals was possible for both sides in the trenches of Northern France, as the battlefield crossed the linguistically and culturally diverse German-French region of Alsace-Lorraine.

The airplane was a new invention when war broke out in Europe. Though the device was unproven in war, German commanders recognized that air combat and aerial bombardment were the most significant war tactics of the future. Britain developed fighter squadrons of its own to combat the German air menace. Despite the fame of the German Red Baron and World War I aerial dogfights, airpower was a very small part of the war effort on both sides. However, low-flying airplanes proved invaluable surveillance and intelligence tools, permitting military command to obtain accurate and up-to-date information on enemy trench locations and fortifications. British forces experimented with aerial surveillance photography, trying several cameras, but the medium had little success during the course of World War I.

German and Austrian forces introduced the use of balloons to monitor weather patterns and deliver explosive charges. Sometimes, dummy balloons were sent across enemy lines so that scouts could monitor where individual balloons were shot down, thus mapping probable enemy strongholds. British and French forces soon reciprocated by using balloons of their own, but by the time they introduced the devices, balloons signaled the impending use of a far more sinister weapon, poison gas.

**Chemical weapons.** Although military strategists during the nineteenth century noted the potential use of poison gas on the battlefield, the development of the first, World War I-era chemical weapon happened by accident. Seeking to

conserve TNT, British and German forces substituted two different agents, Lyddite and Dianisidine salts respectively, into their explosive charges. The chemicals produced a tearing agent and mild respiratory irritant, sending victims into violent fits of sneezing.

The French first developed strong tear gas agents for battlefield use in June 1914. French forces first employed the gas in the form of tear-gas grenades, in August 1914. German scientists created a similar agent, and were the first to research various types of poison gas for extensive battle use. In October 1914, the Germans fired the first gas-filled shells. A few months later, experiments with filled shells were unsuccessful. Gasses failed to properly vaporize on the Eastern Front during the freezing winter. Variable winds on the Western Front made dispersal of gasses difficult.

By 1915, the German, French, and British armies all sought to develop chemical agents that would help end the relentless stalemate of trench warfare. Outdated battlefield tactics ordered soldiers to charge fortified trenches, across open fields strewn with barbed wire. Military commanders hoped poison gas would help soften or destroy manned defenses, permitting successful seizure of enemy positions.

The first major use of strong poison gas was an asphyxiant and respiratory irritant, chlorine, at the Second Battle of Ypres. German forces mounted a heavy bombardment of the French, British, and Algerian Ypres Salient. In the evening, the firing grew more intense, and Algerian troops noticed a peculiar yellow cloud drifting toward the Salient. French military commanders believed the yellow smoke hid an oncoming German advance, so soldiers were ordered to stand their ground and man machine gun defenses. As a result, many men died and the Salient was broken, forcing the Allies to retreat.

Germany drew immediate criticism for its inhumane use of gas on the battlefield. German diplomats assured rival powers that poison gas would be used regularly against their forces, provoking further condemnation. Both sides of the conflict employed agents of espionage to spy on the production of new weapons. Informants told Allied authorities about the possible German use of chlorine gas at Ypres. After Ypres, intelligence personnel changed its tactics to obtain specific information on the gasses each side was producing, and how they intended to weaponize the chemicals.

The British government commissioned Special Gas Companies to create poisons for wartime uses. On September 24, 1915, Allied forces retaliated the initial German gas attacks. Setting some 400 chlorine gas canisters along the German lines at Loos, British forces began the gas attack at dawn. A few minutes after sunrise, the prevailing winds suddenly shifted, driving the cloud of gas back over British lines. The operation was disastrous, Britain suffered more casualties on the day than did Germany.

After the incident at Loos and several similar gas reversals, both British and German forces experimented

with different means of delivering poison gasses to minimize friendly-fire exposure to the chemicals. The creation of stronger, more deadly agents, such as Phosgene (an asphyxiant) and later Mustard Gas (a blister agent that burned exposed skin and eyes), necessitated a remote delivery system. Gas canisters were dropped from balloons and airplanes, but the system was not always reliable and targeting specific locations was difficult. Advancement in ammunition design, and the chemical agents themselves, finally permitted chemical agents to be placed in the payload of long-range artillery shells.

Despite more efficient delivery mechanisms, chemical warfare eventually became less effective on the battlefield. All armies in the conflict quickly devised protective gear to shield soldiers from exposure to chemical agents. Cotton wraps dipped in baking soda and gas masks greatly reduced the number of casualties from most gasses, though they offered no protection from the increasingly used Mustard Gas. Battlefield toxins became more deadly, especially with the limited use of cyanide derivatives and prussic acid, a crippling nerve gas. However, protective clothing and gas masks limited mortality from rare gasses.

Better intelligence also helped combat casualties incurred from gas attacks. Intelligence aided troops in the trenches to reposition to avoid an impending attack. Identification of the type of gasses possessed by the immediate enemy corps further detracted from the element of surprise, upon which gas attacks heavily relied. Despite its diminished success, gas continued to be regularly deployed.

**The legacy of World War I.** By the end of World War I, over 100,000 people were killed, and one million injured, by poison gas attacks. Those injured often suffered debilitating injuries, creating further public ire for chemical weapons. Civilians were inadvertently injured by contaminated areas, especially by the long-lingering mustard gas. After the war, the newly established League of Nations moved to amend the international rules of engagement to disallow the use of poison gas. Though the motion gained public and diplomatic support, military leaders were hesitant to agree to a total ban on chemical warfare. In 1925, the Geneva Protocol outlawed the use of chemical and biological weapons in war against human targets. However, the treaty did not prevent their further use, and chemical and biological weapons attacks by rogue nations or terrorist organizations have now reemerged as a global threat.

The Armistice created the political map of Europe that sparked the powder keg of World War II. The German government collapsed under the weight of reparation payments and hyperinflation, only to emerge from economic troubles under the reign of Adolf Hitler and his Nazi Party. In the East, small ethnic nations were combined into larger states, embittering nationalists that hoped the war would bring freedom from Austrian, Russian, or German domination. Russia began a tumultuous revolution in

1917, withdrawing from the war to concentrate on domestic affairs.

The legacy of World War I extends beyond World War II, however. Many nations participating in the conflict realized the necessity for some sort of permanent intelligence services, whether cryptology and surveillance units, or large government intelligence agencies. The nature of war, and the business of intelligence in wartime and peacetime were altered by the events of World War I.

## ■ FURTHER READING:

### BOOKS:

Gilbert, Martin. *The First World War: A Complete History*. New York: Henry Holt, 1996.

Keegan, John. *The First World War*. New York: Vintage Books, 2000.

### SEE ALSO

*Black Tom Explosion*

*Room 40*

*World War I: Loss of the German Codebook*

# World War I: Loss of the German Codebook

■ ADRIENNE WILMOTH LERNER

At the outset of World War I, the science of cryptography assumed a distinctly modern character. New developments, such as the international telegraph system and the telephone left cryptologists grappling with new ways to adapt encryption methods to the new technology. The ultimate goal of cryptologists of the era was to invent a means of transcribing and decoding ciphers without the use of cumbersome codebooks that could easily fall into enemy hands. Wartime experimentation proved impractical, so for most of the war, both sides relied on older-style codebooks. For the Germans, this proved disastrous. Between 1914 and 1918, the German forces lost four codebooks, all of which were recovered by British intelligence services. For much of the war, German communications were intercepted and deciphered by the British intelligence code-breaking unit known as Room Forty, giving Allied forces a decisive strategic advantage.

The first copy of a German codebook to be recovered by British forces was stolen with the help of British-born Austrian spy, Alexander Szek. Szek was a telegraph operator in Belgium. Room Forty picked up strange signals coming from Szek's station, then contacted Szek, along with locating his relatives in London. British agents sent a letter to Szek, urging him to join the British war effort as a

spy, or face unforeseen consequences. They further threatened to incarcerate his relatives who lived in London.

Szek agreed to help steal German codes by photographing the German codebook. He was intensely nervous about his espionage role for the beginning of the operation, but became even more unnerved as time progressed. Fearing capture by the Germans, Szek arranged with intelligence officers to flee to Britain after he completed his work photographing the codebook. When Szek delivered the last copies of the codebook to an agent in the Netherlands, however, he was returned to Brussels so as not to appear suspicious to German authorities. If the Germans suspected that Szek had stolen the code, the code would be replaced. His jumpy actions rendered Szek a security risk.

Szek was later found shot to death in his apartment in Brussels. The British government claimed that German agents killed Szek after discovering his espionage activities. Unaware of the theft, the Germans continued to use the code Szek had stolen. Some years later, British Navy captain and intelligence attaché Captain Stephen Roskill, admitted to ordering a hired hit on Szek. The British Admiralty was plagued by Szek's constant nervousness and worried that he might confess his actions to the Germans in order to assuage his sense of guilt. Although the information gained from Szek's work was immensely valuable, its price would soon seem exceedingly steep. A few months after incident with Szek, British divers recovered a box from a sunken German U-boat. The box contained a copy of the German Foreign Office code book, the same code that had been laboriously photographed and smuggled to British intelligence by Szek.

1914 was a providential year for Room Forty. In August, a third German codebook, the naval code, was given to British cryptologists by Russian forces. The German cruiser Magdeburg sank off the coast of Finland, and a Russian vessel picked up survivors of the downed ship. Upon searching the German crew, Russian authorities discovered the codebook in the possession of one of the ship's officers. After analyzing the new codebooks, British intelligence was able to decipher and monitor most German fleet dispatches from 1915 to 1917, after which a variant code was introduced.

Room Forty cryptologists received one final gift in 1915. As British forces closed in on Persia, German consul Wilhelm Wassmus hastily fled his office, leaving behind his copy of the German diplomatic codebook. While the code was less frequently used than others, the recovery of the fourth code book gave Room Forty the mathematical key to the main German encryption system.

With a network of listening stations established in Europe and in the North Sea, Room Forty monitored most German wire traffic throughout the course of the war. The loss of codebooks diminished Germany's capability for surprise attacks at sea, despite the advantage of a technically superior fleet. In 1918, the German company Siemens,

under contract with the German government, developed a prototype cipher machine that encoded and decoded messages without need of a codebook.

#### ■ FURTHER READING:

##### BOOKS:

Gilbert, Martin. *The First World War: A Complete History*. New York: Henry Holt, 1996.

Khan, David. *The Codebreakers: The Story of Secret Writing*. New York: Scribner, 1996.

##### SEE ALSO

Room 40

---

## World War II

---

#### ■ JUDSON KNIGHT

The Second World War was history's largest and most significant armed conflict. It served as the breeding ground for the modern structure of security and intelligence, and for the postwar balance of power that formed the framework for the Cold War. Weapons, materiel, and actual combat, though vital to the Allies' victory over the Axis, did not alone win the war. To a great extent, victory was forged in the work of British and American intelligence services, who ultimately overcame their foes' efforts. Underlying the war of guns and planes was a war of ideas, images, words, and impressions—intangible artifacts of civilization that yielded enormous tangible impact for the peoples of Europe, east Asia, and other regions of the world.

### Scope and Consequences of the War

The war pitted some 50 Allied nations, most notable among which were the United States, United Kingdom, Soviet Union, and China, against the Axis nations. The name "Axis," a reference to the straight geographic line between the capital cities of Rome and Berlin, came from a pact signed by Germany and Italy in 1936, to which Japan became a signatory in 1940. Ultimately a number of other nations would, either willingly or unwillingly, throw in their lot with the Axis, but Germany and Japan remained the principal powers in this alliance.

Although the roots of the conflict lay before the 1930s, hostilities officially began with the German invasion of Poland on September 1, 1939, and ended with the Japanese surrender to the United States six years and one day

later. The war can be divided into three phases: 1939–41, when Axis victory seemed imminent; 1941–43, when Axis conquests reached their high point even as the tide turned with the U.S. and Soviet entry into the war; and 1943–45, as the Allies beat back and ultimately defeated the Axis.

Over those six years, armies, navies, air units, guerrilla forces, and clandestine units would fight across millions of square miles of sea and land, from Norway's North Cape to the Solomon Islands, and from Iran to Alaska. The war would include more than a dozen significant theatres in western Europe, the north Atlantic, Italy, eastern and southern Europe, Russia, North Africa, China, southern Asia, Southeast Asia, and the Pacific islands. Less major, but still significant, engagements took place in East Africa, the Middle East, and West Africa. There were even extremely limited engagements—mostly at the level of diplomacy, espionage, or propaganda—in South America and southern Africa.

**Death toll.** World War II and its attendant atrocities would exact an unparalleled human toll, estimated at 50 million military and civilian lives lost. Combat deaths alone add up to about 19 million, with the largest share of this accounted for by 10 million Soviet, 3.5 million German, 2 million Chinese, and 1.5 million Japanese deaths. (The United States lost about 400,000, and the United Kingdom some 280,000.)

Adolf Hitler and the Nazis killed another 15.5 million in a massive campaign of genocide that included the "Final Solution," whereby some 6 million Jews were killed. Another 3 million Soviet prisoners of war, along with smaller numbers of Gypsies, homosexuals, handicapped persons, political prisoners, and other civilians rounded out the total. Principal among the Nazi executioners was the SS, led by Heinrich Himmler, which operated a network of slave-labor and extermination camps throughout central and eastern Europe.

About 14 million civilian deaths have been attributed to the Japanese. They imposed a system of forced labor on the peoples of the region they dubbed the "Greater East Asia Co-Prosperity Sphere," and literally worked millions of civilians and prisoners of war (POWs) to death in their camps. The Japanese also conducted massacres of civilians that rivaled those undertaken by the Nazis in Russia.

Soviet non-combat atrocities accounted for another 7 million deaths. Victims included members of deported nationalities, sent eastward to prevent collaboration with the Nazis; murdered German POWs; returning Soviet POWs killed because of their exposure to the West; and other campaigns of genocide conducted by Soviet dictator Josef Stalin.

World War II served as a watershed between the multi-polar world of the nineteenth and early twentieth centuries, and the bipolar world of the Cold War. It ended the military dominance of European powers, but also



An American medical officer examines the bullet-riddled bodies of three German spies who died before a U.S. firing squad in Herbesthal, Belgium, in December 1944. ©BETTMANN/CORBIS.

ushered in an era in which Europe, heavily aided in its recovery by the United States so as to avoid another European war, became a major economic power.

The war transformed the United States from an isolationist giant, with little interest in affairs outside the Western Hemisphere, to a modern superpower. Symbolic of this transformation was the construction of the Pentagon building, commenced just before the United States entered the war. The war also marked the birth of the modern U.S. intelligence apparatus, of which the Office of Strategic Services (OSS), led by Major General William Donovan, was the progenitor. OSS would cease to function soon after the war's conclusion, but two years later, it would be replaced by a far more lasting organization, the Central Intelligence Agency (CIA).

Despite the wartime alliance with the Soviet Union, and the creation of the United Nations in an effort to settle international differences peacefully, the Cold War was an all but inevitable result of the war, which left only two superpowers in its wake. Thenceforth, the world would be divided between the United States and its allies—among which would be its two wartime enemies, West Germany and Japan—and the Soviet Union and its affiliates. These would include East Germany and eastern Europe; Communist China from 1949 to the Sino-Soviet rift of the late

1950s; and a number of states in the gradually emerging developing world of the Middle East, Africa, and Asia.

The conflict spelled an end to the European colonial empires, and brought independence to dozens of countries in the Middle East, Africa, and south and east Asia. Among the many states that owed their existence to the war was Israel. The effects of the Holocaust moved Western leaders to action, and Western sympathy helped ensure support for the establishment of a Jewish state.

## The Axis and the Causes of the War

The victory of Benito Mussolini's Black Shirts in Italy in October 1922, introduced the world to Fascism, which reinterpreted nationalism in totalitarian terms, i.e., as an all-encompassing political movement intended to supplant all other centers of influence, such as religion, in the life of the individual. Hitler regarded Mussolini as a mentor, yet the Nazis would eclipse the Fascists in terms of strength, influence, and impact on world history.

Not only was Germany's militarily more powerful than Italy's, but the agenda of the Nazis, who took power in January 1933, had a much greater sense of urgency.



Poster designed by artist Cliff Parks for Air Cadets at Ellington Field, Texas, the world's largest multi-motor flying school, in 1942. ©BETTMANN/CORBIS.

Central to Hitler's plans, outlined in his manifesto *Mein Kampf* (1924), was the elimination of central and eastern European Jews, who Hitler regarded as the principal barrier to German European dominance. Intimately tied with this plan was his vision of conquest and colonization in Russia and eastern Europe, which would—after the Jews and Slavs had been exterminated—constitute a German empire or *reich* that Hitler predicted would last a thousand years.

This consciously millenarian vision drew on German history and national mythology, citing as the first and second *reichs* the Holy Roman Empire of the Middle Ages and the German Empire of 1870–1918 respectively. It appealed not only to longstanding strains of anti-Semitism in Europe, which dated back at least to the time of Crusades, but also to disaffection with what the Germans regarded as their betrayal and humiliation in World War I and with the Versailles Treaty of 1919. In a country that had recently been devastated by inflation—Germany's economic crisis preceded the worldwide Great Depression by several years, and was even more severe—Nazism seemed to offer a solution for strengthening a once-great nation that had fallen on difficult times.

**Communism and the Spanish Civil War.** At a rhetorical and symbolic level, Hitler opposed Communism, and used the threat of Soviet Russia as justification for his moves to arm Germany in the 1930s. In reality, the Nazis and Soviets provided one another with mutual assistance, continuing a pattern begun in World War I, when imperial Germany had aided V. I. Lenin. After the war, German aristocrats, nationalists, and Communists all opposed, and helped bring down, the liberal democratic Weimar Republic. Though Hitler killed thousands of Communists after he gained power in January 1933, German military forces trained in Russia, and Germany provided Russia with equipment.

This secret relationship would become public when the two sides signed the Non-Aggression Pact on August 23, 1939, but until that time, Hitler and Stalin made much of their putative opposition to one another. The Spanish Civil War (1936–39) provided them with a proxy battleground, as Germany and Italy tried out new armaments in support of the Nationalists, led by Francisco Franco. The Republican side turned to Stalin for help, but he gave them little assistance while siphoning resources and leaders, some of whom went to Moscow and never returned.

On the other hand, the romance and mythology of the Republican cause provided the Soviets with a propaganda victory that comported well with their current "Popular Front" strategy. In accordance with the latter, Communists worldwide ceased calls for world revolution, and instead formed alliances with liberal, socialist, and anarchist movements. Later, Stalin would form a "popular front" on a grand scale, as he aligned himself with the United States and Great Britain.

**Munich and Mussolini.** Hitler's rhetorical opposition to Communism won him tacit support from Britain and France, which in the 1930s regarded Nazism as the lesser of two evils. At Munich in September 1938, British and French complicity yielded Germany title to a portion of Czechoslovakia known as the Sudetenland. In the view of many historians, the Munich conference and the appeasement efforts of British Prime Minister Neville Chamberlain rendered war all but inevitable.

Munich also sealed the relationship between Mussolini and Hitler. Despite their later alliance, Mussolini, a former Communist, rightly perceived significant differences between his nationalism and Hitler's racism. If Britain and France perceived Hitler as a buffer against Stalin, then Mussolini in the early 1930s seemed like a buffer against Hitler. What brought Italy and Germany together was the same complex of factors that eventually forged a three-way alliance with Japan: a shared desire for greater power, territorial ambitions that had supposedly been frustrated by the democratic powers, and a string of diplomatic and military successes that encouraged ever bolder moves.

**Japan, militarism, and expansionism.** When its troops marched into Manchuria in 1931, Japan launched the first in the series of conquests and invasions during the 1930s that set the stage for the war. Though nominally led by an emperor, Hirohito, by that time the nation had come under the control of military officers, who had imposed a dictatorship. The Japanese lacked a single powerful leader until Hideki Tojo emerged at the top in 1941.

Although certainly authoritarian and strictly controlled, the Japanese system was technically not totalitarian, in the sense that it did not have a specific, animating modern ideology. Instead, it relied on ancient national myths, combined with an abiding sense that Japan had been wronged in its struggle to make a place for itself as a world power. The Japanese belief system combined nationalistic and racial themes: like the Nazis, they regarded all other peoples as inferior. This would have seemingly made the Japanese and Nazi systems mutually exclusive, but because they were at opposite sides of the world, it provided a convenient formula for dividing the planet between them.

Each of the three future participants in the Axis Pact set out to test the resolve of the other powers to oppose them, and found such opposition all but nonexistent. The League of Nations, formed to put an end to wars after World War I, failed to act decisively when Italy conquered Ethiopia in 1935–36, when Germany occupied the Rhineland in 1936, when Japan conquered most of eastern China in 1937–38, or when Germany annexed Austria in 1938.

**1939–41: The Axis triumphant.** Over the course of the first nine months of 1939, Germany added the rest of Czechoslovakia, while Italy occupied Albania. Having signed the Non-Aggression Pact with Stalin in August, Hitler invaded Poland on September 1. Britain and France, which on

March 29 had pledged to support Poland, declared war, but did not attack Germany. During the next few weeks, Germany and Russia divided Poland between themselves, and in November, the Soviet Union launched a separate war with Finland.

Although the Soviets eventually emerged victorious in March 1940, the Russo-Finnish War convinced Hitler of Stalin's vulnerability. Stalin had decimated his officer corps with his purges in the 1930s, and his collectivization efforts had been accompanied by the imprisonment, starvation, and deaths of millions. The Soviet Union was to prove much stronger, however, than Hitler imagined. And if Hitler believed that Japan would join him in making war on the Soviets, he was mistaken; the Soviet performance against the Japanese during the little-known tank battle at Nomonhan in Manchuria in August, 1939, effectively convinced the Japanese of Russia's true strength.

From 1939 to 1941, the Axis unquestionably had the upper hand in the conflict. During the first part of this period, nicknamed "the Phony War," hardly a shot was fired in western Europe. Only in the spring of 1940 did Hitler's forces resume action, conquering Denmark, Norway, the Low Countries, and France. The French, who relied on the defenses of the Maginot Line (designed to fight a World War I-style conflict of limited movement), surrendered after a nominal resistance effort. Most of the country fell under direct Nazi control, which a small portion to the southeast, with the town of Vichy as its capital, formed a pro-Axis government.

The speedy capitulation of the French left the British alone in opposition to the Nazis. In May 1940, Chamberlain resigned, and was replaced by Winston Churchill. In this change, the British people gained an unexpected advantage; over the next five years, Churchill, widely regarded as one of history's great orators, would stir his people to action with a series of memorable speeches. Yet, the position of the British was perilous, and as the Nazi Luftwaffe launched an aerial campaign against them in August, it seemed that German victory was only a matter of time.

**Axis victories and blunders.** At about the same time that the Battle of Britain began, Mussolini attacked the British in North and East Africa. He thus unexpectedly offered England a venue for fighting the Axis outside of Europe, and eventually German forces would be diverted into the Africa campaign.

In southern Europe, Hitler managed to compel Bulgaria, Hungary, and Romania into joining the Axis, but this advantage was overshadowed by another diversion of forces caused by Mussolini. Mussolini invaded Greece in October 1940, and Greek resistance proved so fierce that in April 1941, German forces rolled into southern Europe. Churchill attempted to oppose them in Greece, but the Germans pushed back British forces, and in history's first airborne invasion, took the isle of Crete—an important Mediterranean base—in May.

By mid-1941, virtually all of Western Europe, except Britain and neutral Switzerland, Spain, and Sweden, belonged to the Axis. But the Balkan campaign had pushed back Hitler's timetable for the most important campaign of the war, the invasion of Russia. The purpose of all other fighting up to that point had been to eliminate opposition as Germany invaded the Soviet Union, and rather than conquer Britain, Hitler preferred to enlist it as an ally against Stalin. He called off attacks on British air bases in May 1941, but by then the Nazi bombardment had inflamed British sentiment against Germany.

## 1941–43: The Tide Turns

On June 22, 1941, the Nazis invaded Russia. Operation Barbarossa, as it was called—its name a reference to the twelfth century Holy Roman Emperor Frederick I Barbarossa—was the largest land invasion in history. Fought according to the blitzkrieg ("lightning war") tactics already demonstrated elsewhere in Europe, the invasion relied on mechanized infantry divisions and Panzer (tank) columns with heavy aerial support.

The invasion would initially yield enormous victories for the Nazis, who quickly doubled the size of their territory by annexing most of western Russia. However, the Germans had started the invasion relatively late in the year and were eventually delayed in their advances, given the challenges posed by the Russian winter. This delay was partly due to the incursion into southern Europe, but also resulted from arguments between Hitler and his general staff, which put off the invasion for several weeks.

Not content to be Germany's *Führer* or supreme leader, Hitler also wished to be generalissimo, and eventually he would push aside all military planners and take personal control of the war effort. Not only did Hitler, a corporal in World War I, lack the generals' understanding of strategy, but he tended to be bold where prudence counseled caution, and vice versa. When he had a good chance of taking Britain, he demurred, but a year later, he swept into Russia without taking adequate stock of the consequences.

German troops were not equipped with clothing for the winter. This was in part a consequence of the fact that Hitler resisted apprising his armies or his people of the sacrifices necessary for war. Whereas the Allies immediately undertook rationing efforts, Hitler was slow to enact rationing for fear of unleashing discontent. Likewise, he was ill-inclined to equip his men for a long campaign, and thus admit that such a campaign likely awaited them.

**America enters the war.** Japan launched its first major offensive of the war in early December 1941, when, in addition to attacking the United States at Pearl Harbor, it swept into the Philippines, Malaya, Thailand, and Burma. The result of these decisive attacks, combined with German victories in Russia, was to bring the Axis to the height of its powers in 1942. At that point, it seemed possible that



the two major Axis powers, taking advantage of anti-British unrest in Iran and India, might even link up, thus controlling a swath of land and sea from Normandy to the Solomon Islands.

In actuality, events of 1941 would serve to bring an end to Axis hopes of world conquest. While the invasion of Russia would ultimately cripple the German Wehrmacht, or army, the introduction of the United States to the war would give the Allied force a seemingly bottomless supply of equipment with which to wage the war. It also brought in a vast military force that, alongside the British, would drive back the Germans in North Africa (despite impressive resistance by the tank commander German Erwin Rommel) and make two key landings on the European continent, in Italy and France.

Thus, the attack on Pearl Harbor, intended as a first strike to eliminate American opposition, would prove a miscalculation on a par with Hitler's invasion of Russia. Hitler welcomed the Japanese surprise attack on Pearl Harbor at the time, and quickly declared war on the United States, thus, giving him justification for sinking U.S. ships crossing the north Atlantic in order to deliver supplies to Britain. This proved a benefit to President Franklin D. Roosevelt, who, up to then, had been confronted by strong isolationist opposition to war with Germany.

**1943-45: The Allies victorious.** Unlike the Axis, the Allies were not bound by one single formal alliance. Instead, there were agreements such as Lend-Lease, whereby the United States provided equipment to Great Britain even before it entered the war. Later, America would extend Lend-Lease to the Soviet Union, providing considerable assistance to its future Cold War enemy.

There were also a number of conferences whereby the leaders of the Allied nations planned the postwar world. These included Newfoundland in August 1941, and Casablanca in January 1943, (United States and Britain only), Teheran in November 1943, Yalta in February 1945, and Potsdam in July 1945. (By the latter point, Roosevelt had died and was replaced by Vice-President Harry S. Truman, while Churchill had been voted out in favor of Clement Atlee and the Labour Party.)

As with the Axis alliance of Germany and Italy, there was an alliance within this alliance—that of the United States and Britain. Between Roosevelt and Churchill was a strong personal bond that reflected the ultimate commonality of aims between their two nations. More strained was the relation of these leaders with Stalin. The alliance with Soviet Russia was a marriage of convenience, as all three powers faced a common enemy in Nazi Germany, but Churchill in particular never let down his guard where Stalin was concerned. (And he was right to do so, as Stalin's intelligence services were busy gathering secrets in England.)

To a much smaller extent, the United States and United Kingdom made common cause with the Chinese Nationalists, led by Chiang Kai-shek, and the Free French

under General Charles de Gaulle. In neither case did these leaders speak for their entire nations. Chiang's Nationalists expended greater resources on fighting the Communists, led by Mao Tse-tung, than they did against the Japanese invaders. The Communists, who enjoyed widespread peasant support, proved able defenders, and though they would become enemies of the United States, at the time America regarded them as a useful ally against the Japanese. As for de Gaulle, who operated from London, he represented only a tiny portion of France, most of which made little effort to resist Nazi and Vichy rule.

**Driving back the Axis in Europe.** In Russia, the Germans got as far as the suburbs of Moscow before the winter—along with the resurgent Red Army and a defiant populace—caught up with them. Lengthy sieges at Stalingrad and Leningrad (the latter lasting more than 800 days) would spell an end to German hopes of conquest. Led by Georgi Zhukov, the Red Army gradually drove back the Germans and began the long, steady push into central Europe.

After defeating the Germans in North Africa in late 1942, the Allies invaded Sicily in July 1943, and Italy itself on September 9. This forced Mussolini to retreat to northern Italy, where he would serve as puppet ruler of a Nazi-controlled state for the remaining two years of his life. On June 6, 1944, an Allied force of some 2,700 ships and 176,000 U.S., British, Canadian, and other troops landed at Normandy, in the largest amphibious invasion in history.

By the end of 1944, Allied victory in Europe began to seem all but imminent, but a number of obstacles still stood in the way. Hitler's scientists had developed the V2 rocket, precursor of modern missiles, and Germany fired several of them against England. The Allies, meanwhile, relentlessly bombed German cities, bringing the Reich to its knees. The Battle of the Bulge in the Ardennes forest in December 1944 was the later major Axis offensive in Europe.

With the Soviets surrounding Berlin, Hitler on April 30, 1945, committed suicide in his bunker with his mistress, Eva Braun, along with propaganda minister Josef Goebbels and Goebbels's family. Two days earlier, Mussolini and his mistress, captured by Italian resistance fighters, had been shot. The Germans surrendered to the Allies on May 7. Only after the surrender did the full magnitude of the Holocaust become apparent, and for this and other crimes, those German military and political leaders who did not commit suicide would be tried before the World Court.

**The defeat of Japan.** In the carrier-dominated Battle of the Coral Sea in May 1942, the first naval battle in which opposing ships never caught sight of one another, neither side gained a clear victory, but the Allies won the upper hand at the Battle of Midway the following month. Later that summer, the U.S. Marines fought the Japanese at Guadalcanal in the Solomon Islands, one of the bloodiest battles of the war. Late in 1943, the Marines began a series

of assaults on Pacific islands, including the Gilbert, Marshall, Caroline, and Mariana chains. Allied forces under General Douglas MacArthur liberated the Philippines in the fall of 1944.

Early in 1945, Allied forces under Major General Curtis LeMay began dropping incendiary bombs on Japanese cities, while the Marines took the nearby islands of Iwo Jima and Okinawa. Still, the Japanese resisted, and Allied leaders contemplated a land invasion, to begin in November. The invasion, they calculated, would cost as many as 1 million American lives, with untold casualties on the among the Japanese.

Instead of invading Japan, the United States unleashed the results of the Manhattan Project, which it had begun secretly 1942. Before dropping the atomic bomb, the Allies issued one more plea for the Japanese to surrender, and when they did not, the American B-29 bomber *Enola Gay* dropped a bomb on the city of Hiroshima. Despite the devastation wrought by this, the first use of a nuclear weapon in warfare, the Japanese still refused to surrender. On August 9, the United States dropped a second bomb, this one on Nagasaki. At this point, Hirohito urged the nation's leaders to surrender. Tojo and several others committed suicide, and on September 2, 1945, Japanese representatives formally surrendered.

## A War of Information, Images, and Ideas

The Manhattan Project was the most dramatic expression of a theme that ran through the entire conflict, that ideas and information often contribute as much to a successful military effort as do troops and weapons. Though the First World War brought airplanes into widespread use, along with tanks, and resulted in the popularization of radio soon afterward, the Second World War saw the first true marriage of science and defense to yield the military-industrial complex familiar today. Its legacy is evident in the many technological innovations that were either introduced during its course, or very soon after the fighting ended. In addition to nuclear power and the missile, these include radar, computers, jet engines, and television.

The war also introduced modern concepts of covert and special operations, on the part of the OSS, the British Special Operations Executive (SOE), military intelligence units, and special warfare units that included the Rangers and the precursors to the Navy SEALs of today. The Germans had their spies as well, some of whom even managed to infiltrate the United States, but their efforts in this regard were never as successful as those of the Allies.

**Cryptology.** In the cryptologic war, the Allies were the unquestioned victors. Perhaps the single greatest intelligence success of the war was the British deciphering of the Germans' secret system of communications. Early in the war, British and Polish intelligence officers obtained a

German Enigma cipher machine, to which a team of mathematicians at Bletchley Park applied their expertise. The result was Ultra, the British system for reading the German ciphers.

Thanks to Ultra, the British knew many of the targets in advance during the Battle of Britain. In north Africa in 1942, Ultra helped Field Marshal Bernard Montgomery predict Rommel's actions. So vital was the Ultra secret that the British used it with the utmost of caution, careful not to act too often or too quickly on information it revealed for fear that this might tip off the Germans. Only in the 1970s did the world learn of the Ultra secret.

American successes included the breaking of the Japanese RED cipher by the U.S. Navy, and the PURPLE cipher by the U.S. Army Signal Intelligence Service prior to the war. During the war, the navy proved more successful at breaking the ciphers of its counterpart than did the army. Also notable was the American use of codetalkers transmitting enciphered messages in the Navajo Indian language, which made their transmissions indecipherable to the Japanese. Neither the Japanese nor the Germans scored any major cryptologic victory against the Allies.

**Deception, secrets, and covert operations.** The Allied invasion of Italy was accompanied by a number of behind-the-scenes moves. Just before the invasion of Sicily, British naval intelligence obtained the body of a man who had recently died, and arranged for his body—clad in the uniform of a major in the Royal Marines—to wash up on a shore in Spain. On his person were documents laying out a British plan for an imminent invasion of the Balkans, information the British knew the Germans (who had numerous agents in Spain) would acquire. The ruse, known as Operation Mincemeat (subject of the 1953 film *The Man Who Never Was*) left the Germans unprepared for the subsequent invasion.

The surrender of most of Italy by Marshal Pietro Badoglio appears to have been the result of behind-the-scenes talks with the Allies. During the moments of turmoil in the capital as Mussolini's government was overthrown, a British intelligence officer provided Badoglio with a safe haven. In 1945, Allen Dulles—future director of the CIA—secretly negotiated with SS General Karl Wolff for the surrender of all German forces in Italy.

Another deception campaign, known as Bodyguard, preceded the Normandy invasion of June 1944. Using German agents in England who had been turned by British intelligence, the Allies conducted an elaborate campaign designed to convince the Germans that they were attacking anywhere but Normandy. Radio transmission from Scotland seemed to indicate a thrust toward Norway, while the appearance of Montgomery near Gibraltar suggested an invasion through Spain. (In fact "Montgomery" was actually a British actor who resembled the general.)

The Normandy deception included the creation an entire unit, the First U.S. Army Group (FUSAG), from thin

air. FUSAG, which was supposed to be landing at Calais rather than Normandy, had a putative commander in General George S. Patton, fresh from victories in North Africa and Italy. Large tent encampments created the illusion of massive troop strength, while fake tanks, landing craft, and other equipment gave indications that the Allies were gearing up for a major operation. So, too, did radio communications from Patton’s headquarters, as well as a heavy Allied bombing campaign over Calais in the days leading up to June 6. The ploy succeed in diverting 19 German divisions from Normandy.

The race to develop an atomic bomb involved several covert operations, including British sabotage directed against Nazi weapons materials in Norway, as well as an intelligence-gathering operation known as Alsos. The name was chosen by Major General Leslie Groves, who oversaw the Manhattan Project, because *alsos* is Greek for “grove.” Members of the Alsos team, which included both U.S. Army and Navy personnel, scoured research laboratories in Germany, Italy, France, and Belgium for information on Axis bomb-making efforts.

**Propaganda.** At the simplest level of ideas, propaganda—though a feature of wars since the beginning of history—played a particularly significant role in the Second World War. Its importance to the Nazis is symbolized by the fact that in his final hours, Hitler had Goebbels beside him. Goebbels, who like Mussolini was a former Communist, had powerful instincts for making appeals to the populace, using all available media, including print, radio, and film. (The Nazis even conducted early experiments with television.)

Films by Leni Riefenstahl in the 1930s romanticized the myth of Aryan superiority, while cruder propaganda from Goebbels’ office excited hatred toward Jews. During the war, Axis powers on both sides of the world made considerable use of radio through broadcasters such as Lord Haw Haw (a.k.a. William Joyce), Axis Sally (Mildred Gillars, an American), and a number of Asian females collectively dubbed “Tokyo Rose” by U.S. forces. The Allies conducted a propaganda war of their own, through radio broadcasts and the efforts of the U.S. Office of War Information and the Voice of America.

■ FURTHER READING:

BOOKS:

Breuer, William B. *Undercover Tales of World War II*. New York: J. Wiley, 1999.

Farago, Ladislas. *The Game of the Foxes: The Untold Story of German Espionage in the United States and Great Britain during World War II*. City: Publisher, 1971.

Persico, Joseph E. *Roosevelt’s Secret War: FDR and World War II Espionage*. New York: Random House, 2001.

Shirer, William. *The Rise and Fall of the Third Reich*. New York: Simon and Schuster, 1960.

West, Nigel. *A Thread of Deceit: Espionage Myths of World War II*. New York: Random House, 1985.

SEE ALSO

*Army Security Agency*  
*Cameras*  
*Cold War (1945–1950), The start of the Atomic Age*  
*COMINT (Communications Intelligence)*  
*Cryptology, History*  
*Enigma*  
*FBI (United States Federal Bureau of Investigation)*  
*FISH (German Geheimschreiber Cipher Machine)*  
*French Underground during World War II, Communication and Codes*  
*Germany, Intelligence and Security*  
*Gestapo*  
*Italy, Intelligence and Security*  
*Japan, Intelligence and Security*  
*Korean War*  
*OSS (United States Office of Strategic Services)*  
*Pearl Harbor, Japanese Attack on*  
*RADAR*  
*Red Orchestra*  
*Room 40*  
*SOE (Special Operations Executive)*  
*Soviet Union (USSR), Intelligence and Security*  
*Special Relationship: Technology Sharing between the Intelligence Agencies of the United States and United Kingdom*  
*Truman Administration (1945–1953), United States National Security Policy*  
*Ultra, Operation*  
*United Kingdom, Intelligence and Security*  
*Vietnam War*  
*World War I*  
*World War II, The Surrender of the Italian Army*  
*World War II, United States Breaking of Japanese Naval Codes*  
*World War II: Allied Invasion of Sicily and “The Man Who Never Was”*

World War II: Allied Invasion of Sicily and “The Man Who Never Was”

■ ADRIENNE WILMOTH LERNER

As the World War II Allied campaign in North Africa drew to a close, Allied command turned its attention to its next major objective, an invasion of Europe. From their position in North Africa, with the aid of their fleet in the Atlantic and Mediterranean, the next logical targets for the Allies were German defenses on the Italian island of Sicily.

However, rough terrain and solid German land and air defenses would make a direct assault on the island costly, and potentially disastrous. As the German command expected the Allies to attack Sicily, Allied intelligence was charged with devising a plan to feed misinformation to the Germans, causing them to believe that Allied forces were massing to invade Europe via Greece or the Balkans. The plot became known as “Operation Mincemeat,” or “the man who never was.”

Two British intelligence agents, Ewen Montagu and Sir Archibald Cholmondley, members of the XX “double cross” intelligence committee, proposed to use a dead body, dressed as a military courier, to slip false information about Allied battle plans to the German intelligence service, the Abwehr. The two men convinced Allied command that, with enough attention to the ruse courier’s body, uniform, placement, and personal effects, Abwehr agents were sure to believe the validity of any information the courier carried. The team was given less than three months to carry out the “man who never was” operation.

Montague first located a suitable body, that of man in his 30s who had died of pneumonia. Since the team planned to deliver the body by sea, making it look as though the victim washed ashore after a plane crash, the similarity of the pathology of pneumonia and drowning was highly convenient. After gaining the consent of the dead man’s family, the body was kept in cold storage while a the XX intelligence team went to work on “Operation Mincemeat,” creating a false identity and personal effects for their mystery soldier.

The XX team dressed the body in a Royal Marine uniform, and stuffed his pockets with typical soldier accoutrements. Because the corpse’s false identity would have to appear in public casualty notices printed in the newspapers, the corpse was given the most common name on British military rolls, (acting Capt.) William Martin. Montague and Cholmondley convinced their secretary to write letters to Martin, posing as his fiancée. They included her picture in “Mincemeat’s” pockets.

After producing the false documents and private communications between field generals that were added to Martin’s attaché case, the body was ready to transport, via submarine, to the Spanish coast. The team chose the location because of the plethora of German agents working in the region. In addition, it gave the illusion that the courier was trying to avoid travel over hostile territory. The body was released into the water off the coast of Spain on April 19, 1943. A fishing boat retrieved the remains of the “man who never was,” and reported the find to German agents.

Immediately, British intelligence published William Martin’s name on public casualty lists, with the explanation of missing, presumed dead in air accident. Intelligence officers knew that Abwehr agents would check public records to confirm the man’s identity. To further the deception, the XX team held a mock funeral for Martin

back in England, complete with flowers and a grieving fiancée.

British military intelligence cryptanalysis staff at Bletchley Park monitored German Enigma encoded messages almost in real time. Intercepts indicated that Martin had been found and that the Abwehr had located the misinformation planted on the corpse. Remarkably, within weeks, intercepts revealed that the German High Command had distributed the information to Generals in the Mediterranean. On May 12, 1943, the Germans moved thousands of troops, airplanes, and weaponry from Sicily to fortify defenses in Sardinia and Greece, where they presumed Allied forces were going to invade.

Allied forces invaded Sicily on the morning of July 9. Operation Mincemeat succeeded in weakening German outposts on the island, and allowed the Allies to sweep ashore with astonishing surprise. Though fighting persisted on the island for a month, the clever deception of the “man who never was,” whose true identity has never been revealed, greatly reduced the human cost of the invasion for Allied forces. Sicily fell to Allied control on August 17, 1943.

#### ■ FURTHER READING:

##### BOOKS:

Hinsley, F. H. *British Intelligence in the Second World War*. Cambridge: Cambridge University Press, 1988.

Montagu, Ewen. *Man Who Never Was*. London: Globe Pequot Press, 1997.

##### SEE ALSO

*Bletchley Park  
Codes and Ciphers  
Codes, Fast and Scalable Scientific Computation  
Enigma  
OSS (United States Office of Strategic Services)  
Poland, Intelligence and Security  
Ultra, Operation  
United Kingdom, Intelligence and Security*

---

## World War II, The Surrender of the Italian Army

---

#### ■ JUDSON KNIGHT

The Allied victory in Italy, beginning with the surrender of the Italian government in 1943 and continuing through the conclusion of the war in Europe two years later, was as much a triumph of intelligence, psychological warfare,

and special operations as it was a victory of military might. Among the players in this undertaking were the British Special Operations Executive (SOE), the American Office of Strategic Services (OSS), various units engaged in psychological warfare, and the Italian partisans who fought to regain control of their country.

**Badoglio's capitulation.** By 1943, popular sentiment had long since turned against the Fascist government of Benito Mussolini, but the heavy presence of German troops made the Italians virtual prisoners to the Axis. Faced with this quandary, Prime Minister Pietro Badoglio established clandestine communications with the Allies by diplomatic channels. He thus paved the way for the overthrow of Mussolini on July 25, after which the dictator was arrested. The Allies landed at the beginning of September.

The fact that the fighting in Italy would last until the conclusion of the war—the longest single campaign waged by British and American forces—serves to indicate that matters did not go smoothly even after Badoglio's surrender. A major factor in this was the Germans' resolve to hold on to the northern portion of the country. There, Mussolini (rescued in a daring German airborne raid on September 12) ruled a puppet government, but the real power lay in the hands of the Nazis.

**The Allied effort.** To counter the Nazis' hold on northern Italy, the Allies undertook a number of operations to support the military forces. The latter consisted of the 15th Army Group, commanded by Britain's General Sir Harold R. L. G. Alexander, which included General Bernard Montgomery's British 8th Army, General George S. Patton's U.S. 7th Army, and Lieutenant General Mark C. Clark's 5th U.S. Army. Patton and Montgomery led Operation Husky, the invasion of Sicily in June 1943, while Clark and Montgomery made the first assault on the Italian peninsula three months later.

Assisting this military effort were psychological warfare units of the U.S. 5th Army and the British 8th Army. Klaus Mann, a German American with the 5th Army, designed leaflets intended for the German soldiers. At the same time, OSS was heavily involved behind the scenes. Leading OSS operations was Max Corvo, a Sicilian American who, as a young army private in 1942, had taken a three-day pass to Washington, D.C., and presented a plan for the subversion in Sicily. He soon received a transfer to OSS, and from 1943 to early 1945, Corvo, still in his mid-twenties, ran OSS Italian operations.

At the same time, the Office of Naval Intelligence undertook its own efforts, including one of the most famous (or infamous) aspects of the covert war in Italy: the release of Mafia chieftain "Lucky" Luciano from a Stateside prison to conduct advance work in Sicily. This effectively shut out Corvo who, knowing the Mafia well from his childhood, refused to work with gangsters. Corvo would

later be replaced by James Jesus Angleton, destined to become a major figure in the postwar Central Intelligence Agency. Angleton, a hardline anti-Communist even then, wished to avoid dealing with the Left—a difficult task in a country that had the largest Communist Party of any non-Communist country in Europe. Instead, Angleton ended up working with Masons, syndicalists (non-Communist leftists associated with anarchism), and disaffected Fascists.

**The partisans.** In the shadow war against the Germans, few elements did as much to undermine Nazi power as the Italian partisans, who worked closely with the OSS and the SOE. These Italian irregulars tied up seven German divisions, and forced two of these to surrender, sapping German strength in Italy. With the help of OSS, partisans infiltrated German lines via submarine. Partisan agents such as Mino Farneti set up secret radio communications and arranged parachute drops of weapons to enable a counterattack by partisan forces in the north.

Another partisan aided the escape of five Allied generals who had been captured by the Nazis. In September 1944, a team led by this same operative intercepted and shot a German major traveling by sidecar. In his briefcase they found detailed plans of the Germans' defenses for the eastern half of the Gothic Line. Another partisan smuggled a set of plans for the western half in the sole of his boots, and delivered these to OSS operatives in Siena. Thanks to these plans, the Allied force broke through the Gothic Line on September 17.

#### ■ FURTHER READING:

##### BOOKS:

Chalou, George C. *The Secrets of War: The Office of Strategic Services in World War II*. Washington, D.C.: National Archives and Records Administration, 1992.

Corvo, Max. *The O.S.S. in Italy, 1942–1945: A Personal Memoir*. New York: Praeger, 1990.

Dulles, Allen. *The Secret Surrender*. New York: Harper and Row, 1966.

##### ELECTRONIC:

Prosser, Frank, and Herb Friedman. "Organization of the United States Propaganda Effort during World War II." Psychological Warfare and Aerial Propaganda Leaflets. <<http://psywar.psyborg.co.uk/>> (April 7, 2003).

Tomkins, Peter. "The OSS and Italian Partisans in World War II." Center for the Study of Intelligence, Central Intelligence Agency. <<http://www.cia.gov/csi/studies/spring98/OSS.html>> (April 7, 2003).

##### SEE ALSO

*OSS (United States Office of Strategic Services) Propaganda, Uses and Psychology*  
*SOE (Special Operations Executive) World War II*

## World War II, United States Breaking of Japanese Naval Codes

■ MICHAEL J. O'NEAL

On December 7, 1941, Japanese military forces attacked the United States naval fleet anchored at Pearl Harbor on the Hawaiian island of Oahu. The surprise attack was devastating to the U.S. Navy. Nearly every American plane on Oahu was destroyed; three cruisers, three destroyers, and eight battleships were severely damaged, and two battleships, the *Oklahoma* and the *Arizona* were destroyed; over 2,300 U.S. servicemen lost their lives. In the weeks and months that followed, fears ran deep among shocked Americans that Japan had the ability to launch an invasion on the West Coast of the United States. At the very least, it was feared that the Japanese Navy, facing only the remnants of a tattered American fleet, could effectively control the Pacific Ocean, cutting the United States off from vital resources and shipping lanes.

Over the next three and a half years, in a series of fierce sea and island battles, American forces managed to push the Japanese empire back to its own shores. They were able to do so not only through courage and resolve, but also through the efforts of hundreds of men and women who labored in secrecy, many of them twelve hours a day, seven days a week, cracking the codes that Japanese forces used to transmit messages. Without the information revealed by breaking these codes, the U.S. military could never have countered Japanese offensives throughout the vast expanse of the Pacific, for they would never have known where the Japanese intended to strike next.

**Early code-breaking efforts.** Even before World War I, the United States had been regularly deciphering coded messages sent by foreign diplomats. On the basis of decoded diplomatic messages, for example, the United States and Great Britain knew what arms limitations the Japanese would accept in the peace talks following the war, and negotiators bargained accordingly. The effort to break Japanese diplomatic codes continued into the 1920s and 1930s under the direction of William Friedman, a Russian immigrant who was appointed chief cryptanalyst of the Army Signal Intelligence Service (SIS) in 1922. In the late 1930s, SIS cryptanalysts succeeding in breaking the Purple code, also designated AN-1, which was the principal cipher Japan used to send diplomatic messages. (While the terms code and cipher are often used interchangeably, a code is a substitution of one character or string of characters for another; reading a cipher, however, usually

requires application of some kind of mathematical operation specified by a cipher key; a simple cipher, for example, might require the decoder to subtract a designated value from a string of numbers to arrive at the true string of numbers that encodes a letter, word, or phrase.)

**JN-25.** On June 1, 1939, the Japanese introduced what American cryptanalysts called JN-25. JN means simply Japanese Navy, and JN-25, consisting eventually of about 33,000 words, phrases, and letters, was the primary code the Japanese used to send military, as opposed to diplomatic, messages. After Pearl Harbor, U.S. intelligence efforts focused on cracking JN-25. Leading the effort, code-named Magic, was the U.S. Navy's Combat Intelligence Unit, called OP-20-G and consisting of 738 naval personnel. The unit, housed in the basement of the 14th Naval District Administration at Pearl Harbor, was under the command of Commodore John Rochefort, who combined fluency in Japanese with single-minded dedication to the task. Using complex mathematical analysis, IBM punch-card tabulating machines, and a cipher machine, Friedman had developed the ECM Mark III, the unit was able to crack most of the code by January 1942. The blanket name given to any information gained by deciphering JN-25 was Ultra, a word borrowed from British codebreaking efforts and stamped at the top of all deciphered messages.

The Combat Intelligence Unit worked tirelessly, but the unit had some help from the Japanese themselves. For example, messages, primarily radio transmissions, often began with such stylized phrases as "I have the honor to inform your excellency" and with the names of ships, locations, commanders, the time and date, and similar repeated information that could be easily verified; many referred to military and other officials by formal, stylized titles. These weaknesses, combined with the fact that the Japanese introduced changes to the code only every three to six months, gave American cryptanalysts a toehold into the code. Soon they were able to read the code, which consisted of strings of five digits. Thus, for example, the string 97850 meant submarine, although because JN-25 was really a cipher, the cryptanalyst had to subtract a value from the string of digits to arrive at the correct meaning. Making this task somewhat easier for Americans, the Japanese changed their cipher key infrequently.

**Putting the code to use.** Armed with the ability to read Japanese operational messages, the U.S. Navy was able to turn back the Japanese advance in the Pacific in mid-1942. In April of that year, decrypted messages revealed that Japanese forces were preparing for an assault on Port Moresby, an Australian base in New Guinea, on May 7. In response, U.S. Admiral Chester Nimitz moved his fleet into the Coral Sea between New Guinea and Australia. While the ensuing two-day Battle of Coral Sea was considered a draw, U.S. forces inflicted enough damage on the

Japanese navy to force it to withdraw, giving the United States and Australia time to reinforce Allied defenses in New Guinea.

Perhaps the most dramatic success that resulted from breaking the Japanese naval code was the Battle of Midway in June 1942. The plan of Japanese commander Admiral Isoroku Yamamoto was to assemble an aircraft carrier task force, launch a diversionary raid off the Aleutian Islands, and lure the U.S. Navy to Midway Island and into a decisive battle that would destroy what remained of the American fleet after Pearl Harbor. From decrypted messages, U.S. naval commanders knew the general outlines of the plan, even the timetable. The messages, however, did not say where the Japanese intended to strike; the target was simply designated "AF." It was Rochefort who proposed a ruse to determine what AF stood for. Suspecting that it was Midway Island, he arranged for American forces on the island to send out a radio message saying that they were running short of fresh water. Rochefort and his group waited anxiously to see if Japan would take the bait. Finally, codebreakers intercepted a Japanese message: AF was running short of fresh water. Knowing that the assault was to come at Midway, the U.S. Navy was ready. On June 4, 1942, after a fierce three-day battle, U.S. pilots sank all four Japanese aircraft carriers in Yamamoto's task force, effectively turning the tide in the Pacific. Later, in an unintended breach of wartime security, the *Chicago Tribune* published a story revealing that the navy had known about Japanese intentions in advance, in effect revealing that JN-25 had been broken. The Japanese never found out about the article.

In a postscript to the Battle of Midway, Admiral Yamamoto lost his life as a result of a decrypted message. Codebreakers learned that the admiral was scheduled to inspect a naval base on Bougainville in the Solomon Islands on April 18, 1943. Some U.S. policy makers were hesitant to use this information for fear that doing so would tip off the Japanese that their codes had been broken. Nevertheless, the decision was made to assassinate Yamamoto. That morning, eighteen P-38 fighters left their base at Guadalcanal at the other end of the Solomon chain and arrived at Bougainville just as Yamamoto's plane was making its approach. The admiral was killed in the attack, depriving Japan of its most experienced and accomplished admiral and sapping Japanese morale. To maintain the fiction that the fighters had arrived by chance, the air force flew other patrols in the area, both before and after the attack. The Japanese did not change JN-25, and for the remainder of the war, U.S. intelligence intercepted and read thousands of Japanese messages.

#### ■ FURTHER READING:

##### BOOKS:

Benson, Robert Louis. *A History of U.S. Communications Intelligence During World War II: Policy and Administration*. Washington, D.C.: Center for Cryptologic History, National Security Agency, 1997.

Farago, Ladislas. *The Broken Seal*. New York: Random House, 1967.

Persico, Joseph E. *Roosevelt's Secret War: FDR and World War II Espionage*. New York: Random House, 2001.

Winton, John. *Ultra in the Pacific: How Breaking Japanese Codes & Cyphers Affected Naval Operations Against Japan: 1941-1945*. London: Leo Cooper, 1993.

##### ELECTRONIC:

"Cryptography in the Modern Age." <<http://www.cnn.com/SPECIALS/2001/nsa/stories/crypto.history/>> (January 9, 2003).

Singh, Simon. "US Codebreakers in World War II." <<http://www.vectorsite.net/ttcode7.html>> (January 9, 2003).

##### SEE ALSO

*Cipher Machines*  
*Codes and Ciphers*  
*Cryptology, History*  
*Pearl Harbor, Japanese Attack on*  
*Purple Machine*  
*World War II*

## X-ray Scanners.

SEE *Scanning Technologies*.

## Zimmermann Telegram.

SEE *United States Intelligence, History*.

## Zoonoses

■ BRIAN HOYLE

Zoonoses are diseases of microbiological origin that can be transmitted from animals to people. The causes of the diseases can be bacteria, viruses, parasites, and fungi.

Some zoonotic diseases are identified as potential diseases (e.g., Tularemia) could be exploited by bioterrorists to cause death—including death or contamination of livestock—and widespread economic damage. As of May 2003, the best scientific evidence available suggested that the coronavirus responsible for Severe Acute Respiratory Syndrome (SARS) was originally transmitted from animal hosts.

Zoonoses are relevant for humans because of their species-jumping ability. Because many of the causative microbial agents are resident in domestic animals and birds, agricultural workers and those in food processing plants are at risk. From a research standpoint, zoonotic

diseases are interesting as they result from organisms that can live in a host innocuously while producing disease upon entry into a different host environment.

Humans can develop zoonotic diseases in different ways, depending upon the microorganism. Entry through a cut in the skin can occur with some bacteria. Inhalation of bacteria, viruses, and fungi is also a common method of transmission. As well, the ingestion of improperly cooked food or inadequately treated water that has been contaminated with the fecal material from animals or birds present another route of disease transmission.

A classic historical example of a zoonotic disease is yellow fever. The construction of the Panama Canal took humans into the previously unexplored regions of the Central American jungle.

A number of bacterial zoonotic diseases are known. A few examples are Tularemia, which is caused by *Francisella tularensis*, Leptospirosis (*Leptospiras spp.*), Lyme disease (*Borrelia burgdorferi*), Chlamydiosis (*Chlamydia psittaci*), Salmonellosis (*Salmonella spp.*), Brucellosis (*Brucella melitensis, suis, and abortus*), Q-fever (*Coxiella burnetti*), and Campylobacteriosis (*Campylobacter jejuni*).

Zoonoses produced by fungi, and the organism responsible, include Aspergillosis (*Aspergillus fumigatus*). Well-known viral zoonoses include rabies and encephalitis. The microorganisms called Chlamydia cause a pneumonia-like disease called psittacosis.

Within the past two decades two protozoan zoonoses have definitely emerged. These are Giardia (also commonly known as "beaver fever"), which is caused by *Giardia lamblia*, and Cryptosporidium, which is caused by *Cryptosporidium parvum*. These protozoans reside in many vertebrates, particularly those associated with wilderness areas. The increasing encroachment of human habitations with wilderness is bringing the animals, and their resident microbial flora, into closer contact with people.

Similarly, human encroachment is thought to be the cause for the emergence of devastatingly fatal viral hemorrhagic fevers, such as Ebola and Rift Valley fever. While the origin of these agents is not definitively known, zoonotic transmission is virtually assumed.

Outbreaks of hoof and mouth disease among cattle and sheep in the United Kingdom (the latest being in 2001) has established an as yet unproven, but compelling, zoonotic link between these animals and humans, involving the disease causing entities known as prions. While the story is not fully resolved, the current evidence supports the transmission of the prion agent of mad cow disease to humans, where the similar brain degeneration disease is known as Creutzfeld-Jacob disease.

The increasing incidence of these and other zoonotic diseases has been linked to the increased ease of global travel. Microorganisms are more globally portable than ever before. This, combined with the innate ability of microbes to adapt to new environments, has created new combinations of microorganism and susceptible human populations.

#### ■ FURTHER READING:

##### BOOKS:

Chin, J. "Tularemia." *Control of Communicable Diseases Manual*. Washington, DC: American Public Health Association, 2000.

##### ELECTRONIC:

World Health Organization. WHO Fact Sheets (May, 2003) <<http://www.who.int/health-topics/zoonoses.htm>> (May 12, 2003).

##### SEE ALSO

*Bioterrorism, Protective Measures Infectious Disease, Threats to Security*



*This page intentionally left blank*

## A Compendium of Common Acronyms and Terms

**17 November Organization** Revolutionary Organization 17 November (17 November).

**AAIA** Aden-Abyan Islamic Army.

**AAMVA** American Association for Motor Vehicle Administration.

**ABB** Alex Boncayao Brigade.

**ABI** Airborne Broadcast Intelligence.

**ABM Treaty** The Antiballistic Missile (ABM) Treaty was signed by the United States and the Soviet Union (U.S.S.R.) in 1972. The treaty was one of two treaties produced by the first series of Strategic Arms Limitation Talks (SALT I) between the two countries; the other was an interim agreement limiting offensive nuclear weapons.

**ABMDA** Army Ballistic Missile Defense Agency.

**ABMT** The focus of the Advanced Biomedical Technologies Program (ABMT) is to apply techniques in robotics, virtual reality, three-dimensional visualization, telesurgery, microelectromechanical systems (MEMS), informatics and multi-media simulation to producing products for the care of wounded personnel on the front lines of war.

**Abwehr** The German military intelligence organization from 1866 to 1944.

**ACCES** Advance Cryptologic Carry-on Exploitation System.

**Accommodation Address** An address used by intermediates to transfer messages.

**ACDBU** Automated Counterdrug Database Update.

**ACIPS** Acoustic Intelligence Processing System.

**Acoustic bullets** Scalable low-frequency (10-Hz) sound pulses sent over distances of hundreds of yards, scalable in intensity from painful to lethal.

**Acoustic intelligence** Information derived from audio sources.

**Acoustics** The study of the creation and propagation of mechanical vibration causing sound.

**Active SONAR** Mode of echo location by sending a signal and detecting the returning echo.

**ADARS** Airborne Digital Audio Recording System.

**ADC** Analog to digital conversion.

**ADF** Allied Democratic Forces.

**ADFGX cipher** A code that applies the Polybius square in such a way that the letters *A, D, F, G,* and *X* take the place of numbers for the rows and columns. Some versions, known as the ADFGVX cipher, use the letter *V* to provide additional rows and columns, thus making possible the inclusion of the ten numerals along with the letters of the alphabet.

**ADIO** Australian Defense Intelligence Organization.

**ADSD** Australian Defense Signals Directorate.

**Advanced Encrytion Standard** A cipher algorithm standardized for use by U.S. government agencies and departments.

**AEC** Atomic Energy Commission.

**AEOS** Advanced Electro-Optical System.

**Aerostat** An unmanned, aerodynamically shaped blimp tethered to the ground by a single cable.

**AES** The CryptoAPI algorithm name for the Advanced Encryption Standard algorithm.

**AFI** Air Force Intelligence.

**AFINTNET** Air Force Intelligence Network.

**AFIP** Armed Forces Institute of Pathology.

**AFIS** Automated fingerprint identification systems.

**Aflatoxin** Aflatoxins belong to a group of toxins called mycotoxins, which are derived from fungi.

**AFOSI** The Air Force Office of Special Investigations is the principal investigative service of the United States Air Force.

**AFSA** Armed Forces Security Agency, a forerunner of the National Security Agency.

**Agent** A person hired or recruited by an intelligence agency to do its bidding. Compare with *operative*.

- Agent H blister agent** Mustard bis-(2-chloroethyl)sulfide.
- Agent L** Lewisite: dichloro(2-chlorovinyl) arsine.
- Agent of influence** A person who does not directly work for an intelligence agency, but willingly acts on its behalf to influence public or political opinion.
- Agent orange** A defoliant; that is, a chemical that kills plants and causes the leaves to fall off the dying plants.
- Agent provocateur** An operative or agent who infiltrates a group or organization with the purpose of inciting its members to self-destructive acts.
- Agent Q** Sesquimustard, 1,2-bis-(2-chloroethylthio)ethane.
- Agent T** Agent T bis-(2-chloroethylthio ethyl)ether (potential mustard agent additive).
- Agent-in-place** An employee of one intelligence agency who, of his or her own initiative, offers services to a rival or enemy agency. The agent-in-place continues to work for the first agency, and feed information to the second one.
- AHFWS** Army HF Electronic Warfare System AN/TLQ-33.
- AI** Army Intelligence.
- AIAI** Al-Ittihad al-Islami.
- AIIB** Anti-Imperialist International Brigade.
- Air Force Office of Special Investigations (AFOSI)** The principal investigative service of the United States Air Force.
- Air marshal** United States air marshals are the first police force of the federal government created solely to protect against air terrorism.
- Air plume** A layer of warm air that immediately surrounds a person's body. It has also been referred to as a human thermal plume.
- AIRES** Advanced Imagery Reqs & Exploitation System.
- AIRTAPS** Aerial Imagery Reconnaissance Tracking and Plotting System.
- Aleph** Aum Supreme Truth (Aum) Aum Shinrikyo, Aleph.
- ALG class key exchange** The CryptoAPI algorithm class for key exchange algorithms.
- Algorithm** A method for solving a mathematical problem by using a finite number of computations, usually involving repetition of certain operations or steps. Frequently used in computer science.
- ALIR** Army for the Liberation of Rwanda.
- Al-Qaeda** Responsible for the September 11, 2001, terrorist attacks upon the United States, Al-Qaeda (also known as Al-Qaida) was established by Osama bin Ladin (also spelled Usama Bin Ladin or Osama bin Laden) in the late 1980s to bring together Arabs who fought in Afghanistan against the Soviet Union. Al-Qaeda helped finance, recruit, transport, and train Sunni Islamic extremists for the Afghan resistance. Al-Qaeda's current goal is to establish a pan-Islamic caliphate throughout the world and has declared the United States to be an enemy to be attacked by terrorist actions.
- AM-band** Amplitude Modulated (AM) radio carrier frequencies 535–1605 kHz assigned by the FCC in 10 kHz intervals.
- AM-band (maritime and aircraft navigation frequencies)** Amplitude Modulated (AM) radio carrier frequencies 30 to 535 kHz.
- AMU** Atomic mass units.
- ANNULET** Cryptologic maintenance system.
- ANO** Abu Nidal Organization.
- ANSI** American National Standards Institute.
- ANSIR** FBI Awareness of National Security Issues and Response Program.
- Anthrax** A disease that is caused by the bacterium *Bacillus anthracis*. The bacterium can enter the body via a wound in the skin (cutaneous anthrax), via contaminated food or liquid (gastrointestinal anthrax), or can be inhaled (inhalation anthrax).
- Antibiotics** Agents that kill bacteria. Antibiotics act only on bacteria and are not effective against viruses.
- Antivirals** Compounds that are used to prevent or treat viral infections via the disruption of an infectious mechanism used by the virus.
- Anvil** Automated Target Recognition on Multi-Spectral Imagery.
- APF** Alliance of Palestinian Forces.
- APIS** The Advance Passenger Information System (APIS) is an electronic database system that stores information about airline travelers. The system, operated by the United States Customs Service, the Immigration and Naturalization Service (INS), and the Federal Aviation Administration (FAA), provides searchable biographical and security information on air travelers entering the United States from a foreign destination.
- Apogee** An orbital position where a satellite is farthest from Earth.
- Apogee Kick Motor (AKM)** Satellite rockets that boost a satellite from a temporary orbit to a geostationary (GEO) orbit.
- APS** Advanced Photon Source.
- ARAC** The Atmospheric Release Advisory Capability (ARAC) is an effort through which the United States Department of Energy (DOE) monitors and predicts the release of hazardous materials into the atmosphere.
- Area 51** The popular name of a secret military facility at Groom Lake, Nevada, approximately ninety miles north of Las Vegas. The six-by-ten mile rectangular air base lies within the Switzerland-sized boundaries of Nellis Air Force Base, and has served as a testing ground for "black budget" (top-secret) military prototype aircraft since the mid-1950s. Area 51 is also a well-known folk symbol of an alleged, but scientifically improbable, government conspiracy to cover up information on UFOs and extraterrestrial life.
- AREAS** Airborne Reconnaissance Evaluation and Analysis System.
- ARGUS** Army intelligence database.
- ARPANet** Early DARPA program that led to the development of the Internet.
- Array** A large group of hydrophones, usually regularly spaced, forming a SONAR net.

- ASA** The Army Security Agency (ASA) provided the United States Army with signal intelligence and security information from 1945 to 1976.
- ASARS** Advanced Synthetic Aperture Radar System.
- ASAS** All Source Analysis System.
- ASCI** Accelerated Strategic Computing Initiative.
- ASG** Abu Sayyaf Group.
- ASIO** Australian Security Intelligence Organization.
- ASIS** Australian Secret Intelligence Service.
- Assassination** A sudden, usually unexpected act of murder committed for impersonal reasons, typically with a political or military leader as its target.
- Assay** A determination of an amount of a particular compound in a sample.
- Assessment** Evaluating the potential value of an agent or source.
- Asset** Agents, sympathizers, or supporters that intelligence agencies can exploit to complete mission objectives.
- ASTECS** Advanced Submarine Tactical ESM Combat System.
- Asymmetric warfare** In contrast to traditional warfare or “linear warfare,” asymmetric warfare refers to operations that do not rely on masses of troops or munitions to destroy and/or control an enemy. Asymmetric warfare most commonly refers to warfare between opponents not evenly matched where the smaller or weaker force must exploit geography, timing, surprise, or specific vulnerabilities of the larger and stronger enemy force to achieve victory.
- ATARS** Advanced Tactical Reconnaissance Airborne System.
- ATF** In accordance with the Homeland Security Act of 2002, on January 24, 2003, the Bureau of Alcohol, Tobacco, and Firearms (ATF or BATF) was transferred from the Department of the Treasury to the Department of Justice. There it became the Bureau of Alcohol, Tobacco, Firearms, and Explosives, but retained the initials ATF.
- ATI** Air technical intelligence, or the gathering of intelligence regarding aircraft—as opposed to aerial surveillance or reconnaissance, which is intelligence gathered *using* aircraft. In some cases, aerial operations may be used to gather ATI.
- ATR** Automatic/Aided Target Recognition.
- AUC** United Self-Defense Forces/Group of Colombia (AUC).
- Audio amplifier** Electronic devices that increase the power of an electrical signal whose vibrations are confined to the audio frequency range—the range that can be perceived by the human ear.
- Aum Shinrikyo, Aleph** Aum Supreme Truth (Aum) Aum Shinrikyo, Aleph.
- AUV** An autonomous underwater vehicle, or small, submarine-like robot.
- AVA** Anthrax vaccine adsorbed.
- AVS** Airborne Video Surveillance.
- B-2** The United States Air Force B-2 stealth technology low-observable, strategic, long-range bomber.
- Bacillus anthracis** The bacterium that causes anthrax.
- Back door** An unadvertised portal or route into a secure system.
- Background Investigation** Investigation of individuals who require a security clearance in working with classified documents.
- Bagman** An agent who acts as a paymaster to spies or makes bribes.
- Ballistic fingerprint** The unique pattern of markings left by a specific firearm on ammunition as it is discharged.
- Ballistic missiles** Any missile that lofts an explosive payload, which descends to its target as a ballistic projectile—that is, solely under the influence of gravity and air resistance—is a ballistic missile. Missiles that do not deliver a free-falling payload, such as engine powered cruise missiles (which fly to their targets as robotic airplanes), are not “ballistic.”
- Ballistic transport** Movement of a carrier through a semiconductor without collisions, resulting in extraordinary electrical properties.
- Ballistics** The study of projectile motion, or the motion of objects that have been thrown, shot, or launched. In the context of forensic science, the term usually involves the study of ammunition and firearms.
- Bandwidth** Transponder frequency range/capacity (generally given in MHz).
- Barbiturate** A class of drugs with sedative and hypnotic activities.
- Barnacle** The codename for a specific program within the Special Naval Collection Program (SNCP).
- Barrel (of oil)** The traditional unit of measure by which crude oil is bought and sold on the world market. One barrel of oil is equivalent to 159 liters (42 U.S. gallons).
- Baseline** In triangulation, the measured and known side of a triangle.
- Bathymetric map** Maps that depict the ocean (sea) depth depending on geographical coordinates, just as topographic maps represent the altitude of Earth’s surface in different geographic points.
- BCIS** U.S. Department of Homeland Security, Bureau of Citizenship and Immigration Services.
- BDA** Bomb damage assessment.
- BEADS** Biodetection Enabling Analyte Delivery System.
- BEARTRAP** Acoustic data collection and processing.
- Belly buster hand drill** The “belly buster” hand-crank drill served as an aid to audio surveillance efforts by the United States Central Intelligence Agency (CIA) during the 1950s and 1960s. Designed to drill holes into masonry, the device made it possible to implant audio devices for covert listening.
- BEP** United States Bureau of Engraving & Printing.
- Berlin Tunnel** The Berlin Tunnel involved an attempt by American and British intelligence to adjust to the late 1940s Soviet shift from wireless transmissions to landlines by tapping Soviet and East German communication cables via a tunnel dug below the communist sector of the German city.

- Binary weapon** A chemical weapon in which two harmless agents are stored in separate containers and only mix to form toxic substance on contact with the target.
- BINOCULAR** NSA signals intelligence product.
- BioAPI** Biometric Application Programming Interface.
- Biocontainment laboratories** A laboratory that has been designed to lessen or completely prevent the escape of microorganisms.
- Biodetectors** Analytical devices that combine the precision and selectivity of biological systems with the processing power of microelectronics.
- Bioflips** Specialized microprocessors that can be implanted in the body and that are capable of configuring and calibrating themselves internally via biological feedback (e.g., a response to a set of biological conditions or parameters).
- Biological warfare** As defined by The United Nations, the use of any living organism (e.g. bacterium, virus) or an infective component (e.g., toxin), to cause disease or death in humans, animals, or plants. In contrast to bioterrorism, biological warfare is defined as the “state-sanctioned” use of biological weapons on an opposing military force or civilian population. Biological weapons include pathogenic viruses, bacteria, and biological toxins.
- Biological weaponization** Putting a pathogen in a form or suspension to make it an effective military weapon.
- BioMagnetICs** Bio-Magnetics Interfacing Concepts.
- Biometrics** An automated technique measuring physical characteristics (such as fingerprints, hand geometry, iris, retina, or facial features) of an individual for the purpose of identification or authentication of that individual.
- BIOS** Biological Input/Output Systems program.
- BioShield project** A joint effort between the Department of Homeland Security and the Department of Health and Human Services, Project BioShield is tasked to improve treatment of diseases caused by biological, chemical and radiological weapons.
- Bioterrorism** The use of a biological weapon against a civilian or military population by a government, organization, or individual. As with any form of terrorism, its purposes include the undermining of morale, creating chaos, or achieving political goals. Biological weapons use microorganisms and toxins to produce disease and death in humans, livestock, and crops.
- BIS** (Bezpečnostní Informační Služba) Czech Security Information Service.
- Bitstream embedding** The insertion of message data in digital documents or data streams that contain enough redundancy that some of their information can be altered without obvious effect. For instance, one might conceal a message bitstream inside a digital audio file by replacing the least-significant bit of every waveform sample (or every *n*th waveform sample).
- Black chamber** The term “black chamber” has come to represent any code-breaking organization, but was originally applied to groups of code-breakers associated with a nation’s Post Office that intercepted, read, copied and decoded diplomatic mail.
- Black ops** Shorthand for “black operations,” covert or clandestine activities that cannot be linked to the organization that undertakes them.
- Black September** aka/see: Abu Nidal Organization (ANO).
- Black Tom explosion** The peak act of German sabotage on American soil during the First World War. On July 29, 1916, German agents set fire to a complex of warehouses and ships in the New York harbor that held munitions, fuel, and explosives bound to aid the Allies in their fight.
- BLACKER** NSA end-to-end encryption system.
- Blackmail** The threat to expose an individual’s illegal or immoral acts if the individual does not comply with specific demands.
- Bletchley Park** The headquarters of the British Military Intelligence Government Code and Cipher School during World War II.
- Block cipher** A cipher that transforms fixed-length blocks of plaintext into ciphertext and vice-versa.
- Bludgeon** A general term for any weapon that consists of a short stick with one end weighted. Examples are the black-jack or cosh.
- BMDO** The Ballistic Missile Defense Organization (BMDO), the successor to the Strategic Defense Initiative Organization in the United States Department of Defense, develops systems to detect, track, and destroy ballistic missiles.
- BND** German Bundesnachrichtendienst.
- Bombe** A mechanical device used for the rapid decryption and transcription of complex ciphers. Developed during World War II, the multiple bombes employed by British and United States military intelligence code breakers aided the allied war effort by providing access to German and Japanese military secrets.
- Bomb-grade nuclear materials** Bomb-grade uranium or plutonium is defined as any alloy of uranium or plutonium that is pure enough to be used in bombs.
- Bona fides** An individual’s verified qualifications, credentials, or background history.
- Boost phase** That part of a ballistic weapon’s flight path during which it is being accelerated (boosted) by its rockets.
- BOSS** Bio-Optic Synthetic Systems.
- Botulinum toxin** Botulinum toxin is among the most poisonous substances known. The toxin, which can be ingested or inhaled, and which disrupts transmission of nerve impulses to muscles, is naturally produced by the bacterium *Clostridium botulinum*. Certain strains of *C. baratii* and *C. butyricum* can also be capable of producing the toxin.
- Brainwashing** An attempt to tear down an individual’s former beliefs and replace them with new ones through an intense psychological and sometimes physical process.
- Brain-wave scanner** In conjunction with MRI, brain-wave scanners research is devoted to developing electronic equipment able to predict whether an individual is lying or concealing the truth in statements.
- Brute force** A method of decryption in which a cryptanalyst, lacking a key, solves a cipher by testing all possible keys. This tends to be impractical for most ciphers without the

- use of a computer, and for the most sophisticated modern ciphers, brute force is all but impossible.
- BTS** Directorate of Border and Transportation Security (BTS), Department of Homeland Security.
- Bucket dropper** A spy satellite that takes pictures on film and returns the film to Earth for analysis.
- Bug** Intelligence and security slang for an electronic device consisting of a microphone and a radio transmitter.
- C3** A U.S. Department of Defense abbreviation for command, control, and communications.
- C4** A U.S. Department of Defense abbreviation for command, control, communications, and computers.
- CAM** Chemical Agent Monitoring device.
- Camouflage** Derived from the French *camoufleur* ("to disguise"), the term "camouflage" entered the English language during World War I, when the development of military aircraft exposed troop positions to enemy reconnaissance planes. Camouflage seeks to obscure or "hide in place."
- Candestine information** Information obtained without either the knowledge or consent (e.g. classified or secret information obtained from foreign governments).
- CAP** Continuous assisted performance.
- CAPPS** Computer Assisted Passenger Pre-Screening System.
- CAPS** Computer Assisted Passenger Screening System.
- Carrier battle group** A force of a half-dozen or more ships, with an aircraft carrier as its centerpiece, that includes destroyers, frigates, cruisers, submarines, and supply vessels.
- Carrier current** Transmission of low-frequency radio signals on power or telephone lines.
- Carrier to Noise ratio (C/N)** A ratio used to measure and denote signal quality. The greater the ratio the better the signal.
- Carriers** Charge-carrying particles in semiconductors, electrons, and holes.
- Case** An entire intelligence operation.
- Case officer** An intelligence officer whose job it is to supervise agents working on a case.
- Catalog number** A unique number issued by NASA that identifies a satellite.
- CATIS/IESS** Computer Aided Tactical Information System/Imagery Exploitation Support System.
- CB** Chemical and biological.
- C-band** Multiple channels with horizontal and vertical uplinks and downlinks. Downlinks: 3.720–4.180 GHz; Uplinks: 5.945–6.405 GHz.
- CBEFF** Common Biometric Exchange File Format.
- CBIAC** The Chemical and Biological Defense Information Analysis Center (CBIAC) is a civilian-operated institution that contracts with the United States Department of Defense (DOD) to provide information on chemical and biological warfare technology.
- CBIRF** The Chemical and Biological Incident Response Force (CBIRF) is a unit of the United States Marines devoted to countering chemical or biological threats at home and abroad.
- CBNP** Chemical and Biological National Security Program (CBNP), United States Department of Energy (DOE).
- CCCP** Central Committee, Communist Party, Soviet Union (USSR).
- CCDB** Common Cryptologic Database.
- CCOP** Cryptologic Carry-On Program.
- CCSE** Canadian Communications Security Establishment.
- CCSEW** Canadian Communications Security Establishment.
- CCTV** Closed-circuit television (CCTV) involves the use of video cameras to produce images for display on a limited number of screens connected directly to a non-broadcast transmission system (e.g., a network of cables).
- CDC** Centers for Disease Control and Prevention. The center, which is headquartered in Atlanta, Georgia, is one of the predominant public health institutions in the United States and in the world. The CDC serves United States national security by monitoring the incidence of infectious disease in the United States (and around the world), and through the development and implementation of disease control procedures.
- CDIS** Counter Drug Intelligence System.
- CE** Counter-espionage.
- Cell** Most fundamental or basic unit of a network (e.g. terrorist network).
- Cells** Biology: The smallest living units of the body which together form tissues.
- CERN** Located along the French-Swiss border near the Swiss capital Geneva, CERN is the world's largest particle-physics laboratory. (The acronym stands for Conseil Européenne pour la Recherche Nucléaire, French for CERN's original name, the European Council for Nuclear Research; since October 56, 1954, despite retention of the old acronym, CERN's name has actually been *Organization Européenne pour la Recherche Nucléaire*.)
- CES** Collection Evaluation System.
- CESG** United Kingdom Communications-Electronics Security Group.
- CFF** Cambodian Freedom Fighters.
- CGNRC** Coast Guard National Response Center.
- Chemical warfare** The aggressive use of bulk chemicals that cause death or grave injury. These chemicals are different from the lethal chemical compounds that are part of infectious bacteria or viruses.
- Chernobyl** On April 26, 1986, a nuclear reactor in the town of Chernobyl (in the Ukraine, then a member state of the Soviet Union) exploded, collapsing the building in which it was located and releasing a radioactive plume that deposited material over much of Europe and Scandinavia.
- Chief of mission** The leading representative of the U.S. president in a host nation—usually an ambassador.

- China syndrome** A hypothetical nuclear power plant accident in which the molten uranium of the ruined core will coalesce into a single superheated mass and melt its way down to the groundwater below the plant, causing a violent steam explosion and dispersing even larger quantities of radioactive material.
- Chlorine gas** Lung irritant generally mixed with phosgene.
- Chromatography** Techniques for separating molecules or compounds based on differential absorption and elution.
- CIA** United States Central Intelligence Agency.
- CIAO** Critical Infrastructure Assurance Office.
- CIAP** Command Intelligence Architecture Planning Program.
- CIB** Controlled Image Base.
- CIBS-M** Common Integrated Broadcast Service Modules.
- CIC** United States Counterintelligence Center.
- CIG** Central Intelligence Group.
- CIGSS** Common Imagery Ground/Surface System.
- CI/HUMINT** Counterintelligence/Human Intelligence.
- CIPA** The Classified Information Act, passed by Congress in 1980. CIPA presents guidelines for the use of classified information by both government and defendant in a legal case.
- Cipher** A cipher uses a system of fixed rules (an algorithm) to transform a legible message (plaintext) into an apparently random string of characters (ciphertext).
- Cipher disk** A handheld coding device for generating a limited number of substitution ciphers, that is, ciphers in which each letter of the regular alphabet is enciphered as a single character from a cipher alphabet.
- Cipher key** A sequence of symbols that a user of a given cipher system must possess in order to use the system. Without a key, a user cannot encipher messages (turn them from plaintext to ciphertext) or decipher messages (turn them from ciphertext to plaintext).
- Cipher machine** A mechanical device that assists in the production of ciphertext from plaintext and vice versa. In this broad sense, any mechanical aid from a cipher wheel to a supercomputer can qualify as a cipher machine; however, the term is usually reserved for devices that are fairly complex and that operate on mechanical or electromechanical rather than on electronic principles.
- Cipher pad** A printed list of cipher keys, each intended to be used for the encipherment and decipherment of a single message. Cipher pads (also termed one-time pads) are closely related to one-time tapes and stream ciphers.
- Cipher text** Series of symbols produced by a cipher to convey a message; intended to be unreadable by unauthorized persons.
- Ciphony** The scrambling through technology of the spoken word.
- CIRA** Continuity Irish Republican Army.
- CITA** DOE Counterintelligence Training Academy.
- Clam dead drop** A tiny metal chamber used for concealing materials to be transferred at a dead drop. Attached to the chamber is a magnet, such that it can be attached to an inconspicuous place on a car or any other large object with metallic parts.
- Clandestine operation** A covert or secret operation.
- Clarke belt** A geostationary orbit named for author Arthur C. Clarke, an early proponent of the orbit.
- CLASS** Consular Lookout and Support System.
- Classified information** Materials or data belonging to, controlled by, and/or produced by the federal government, pertaining to intelligence sources or methods of collecting information; cryptology or codes; and the vulnerabilities, capabilities, or planning of systems, installations, or projects that relate to national security.
- Clipper chip** Devices that permit secure encrypted voice communications, but also allow United States law enforcement and intelligence agencies to monitor those communications by obtaining the algorithm keys to decrypt the transmissions.
- CNC** Crime and Narcotics Center.
- Cobbler** A forger of false documents, including identification papers (e.g. passports, visas, birth certificates, etc.).
- Code** A system for concealing a message by replacing words or phrases with symbols. It is distinguished from a cipher in that the latter replaces each letter of a plain-text message, whereas a code replaces entire words or phrases in such a way that there is no one-to-one correspondence.
- Code name** A word or phrase used to refer secretly to a specific person, group, project, or plan of action. Individual spies and large-scale military operations are often referred to by code names to protect their identity.
- Code word** A word or phrase that is used to convey a predefined message that differs from its own literal meaning.
- Codes and ciphers** Forms of cryptography, a term from the Greek *kryptos*, hidden, and *graphia*, writing. Both transform legible messages into series of symbols that are intelligible only to specific recipients. Codes do so by substituting arbitrary symbols for meanings listed in a codebook; ciphers do so by performing rule-directed operations directly on original message text.
- Cognitive computers** Computing systems designed to learn and adapt their programming.
- Coin knife** A small, blunt knife—more effective for the purposes of escape than for inflicting bodily harm—attached to the back of a large coin by a hinge.
- COINS** Community On-line Intelligence System.
- COINTELPRO** (*Conter Intelligence Program*). A set of programs commenced by the United States Federal Bureau of Investigation (FBI) in 1956 and officially terminated in 1971. COINTELPRO included programs variously named Espionage COINTELPRO; New Left COINTELPRO; Disruption of White Hate Groups (targeting the Ku Klux Klan); Communist Party, USA COINTELPRO; Black Extremists COINTELPRO; and the Socialist Workers Party.
- Cold war** An ideological, political, economic, and military conflict primarily between the United States, United Kingdom and Western allies against the Union of Soviet Socialist Republics (U.S.S.R.) and Soviet dominated Eastern bloc

- nations that began in the aftermath of World War II and ended in 1989. From the outset, the cold war was inextricably linked with the development of the atomic bomb and its use as a military deterrent.
- Collection** Obtaining, assembling and organizing information for further intelligence use.
- Colossus I** The world's first programmable computer. Colossus I was created during World War II by the British to speed up the decryption of German messages encoded by the Lorenz Schlüsselzusatz (SZ) 40 and 42 machines.
- COMINT** Communications intelligence, or intelligence gained through the interception of foreign communications, excluding open radio and television broadcasts. COMINT is, along with ELINT or electronic intelligence, one of two subsets of signals intelligence (SIGINT).
- Company, The** The nickname for the CIA (United States Central Intelligence Agency).
- Compartment** A group of individuals with a "need to know," and thus with specialized security access, for a specific topic.
- Comprehensive Test Ban Treaty** An international agreement designed to end the testing of nuclear explosives. As of March 2003, the United States is one of the 166 states that have signed the treaty, but the CTBT will only "enter into force" (i.e., take on the force of law for all ratifying states) when forty-four "nuclear-capable" countries specifically listed in the treaty have all ratified the treaty.
- Compute modeling** Modeling, in the technical use of the term, refers to the translation of objects or phenomena from the real world into mathematical equations.
- Computer Fraud and Abuse Act of 1986** The Computer Fraud and Abuse act served to define criminal fraud and abuse for computer crimes on the federal level.
- Computer keystroke recorder** A program that runs in the background as a computer operates, sequentially recording all keystrokes. Also called a keystroke logger, key logger, or keylogger.
- Computer Security Act of 1987** The first major U.S. government effort to legislate protection and defense for unclassified information in government-related computer systems.
- Computer virus** A program or segment of executable computer code that is designed to reproduce itself in computer memory and, sometimes, to damage data.
- Confidential** The lowest U.S. general security classification. A term referring both to information whose disclosure to unauthorized personnel could reasonably be expected to cause damage to national security, and to the security clearance necessary to access such information.
- Contact** An agent who serves as a liaison.
- Continuous assisted performance (CAP)** Programs that are designed to allow an increase in operation tempo by allowing soldiers to operate without sleep, or limited amounts of sleep.
- Control** The supervising officer or agent.
- CONUS** Continental United States.
- Co-option** The taking over and controlling of a spy from one intelligence service to another.
- Copyright laws** Laws that protect the rights of authors and artists by assuring them the exclusive legal right to reproduce, distribute, perform, display, or license work, as well as derivatives of the work.
- Counterintelligence** The use of intelligence resources to identify, circumvent, and neutralize the intelligence activities of a foreign power.
- Countermeasures** Techniques designed to defeat a defensive system.
- Courier** An agent who retrieves and delivers messages.
- Cousins** A name for the CIA used by British intelligence.
- Cover** A business/trade front which conceals espionage operations.
- Coverage** In electronics use: An area where a signal can be received.
- Covert operations** Activities that are carried out by an intelligence or security agency, usually in a foreign country, in such a way that it is difficult to connect that agency with its action.
- CPNB** Chemical and Biological National Security Program.
- CPSC** Consumer Product Safety Commission.
- Crib** A section of an encoded or enciphered message that can easily be rendered into plain text, thus providing a tool whereby a skilled cryptanalyst can crack the entire code or message.
- Critical infrastructure** A general term for physical and computer-based systems essential to the functions of the government and economy. Among these are telecommunications, energy, banking and finance, transportation, water systems, and emergency services.
- CRS** Comprehensive radiation sensors.
- Cruise phase** Portion of a ballistic missile's flight during which the payload has separated from the booster but has not yet begun to descend toward its target.
- Cryptography** The use of messages concealed by codes or ciphers.
- Cryptology** The study of both cryptography and cryptanalysis.
- Cryptonym** Cryptonyms, or code names, are words, symbols, or numbers used in place of the actual name of a person, item, or planned event.
- Crytanalysis** The breaking of coded messages without prior possession of the key.
- CSE** United States Center for Security Evaluation.
- CSI** The Center for the Study of Intelligence (CSI) of the United States Central Intelligence Agency (CIA) is a reference and resource center for scholars and others studying the history and practice of intelligence disciplines.
- CSIC** Canadian Security and Intelligence Community.
- CSIL** Commercial Satellite Imagery Library.
- CSIS** Canadian Security Intelligence Service.
- CSIS** Center for Strategic and International Studies.
- CT** CT scanners.



- CT product** Mathematical product of concentration (mg/m<sup>3</sup>) multiplied by time of exposure in minutes.
- CTBT** Comprehensive Test Ban Treaty.
- CURV** Cable-Controlled Undersea Recovery Vehicle.
- Customs Service** United States Customs Service (previously part of the Department of Treasury). On March 1, 2003, agents were transferred to the Department of Homeland Security (DHS), directorate of Border and Transportation Security (BTS).
- Cut and cover** A type of underground construction in which a structure is built within an excavated area and then covered with soil or rock.
- Cutout** An agent who serves as a liaison.
- CX** Phosgene oxime or dichloroform oxime.
- Cyber security** Measures taken to protect computers and computer networks from accidental or malicious harm.
- Cyberattack** An assault on the security of a computer system, usually by a hacker or other cybercriminal.
- Cybercrime** Criminal activity involving the use of a computer.
- Cyclosarin nerve agent** GF; Cyclohexyl methylphosphonofluoridate.
- D notice** (defense notice). An alert given by British intelligence services or the armed forces to the media, alerting them of sensitive content that could damage national security or defense if reported in part or in whole.
- DACS** Deportable Alien Control System.
- Dagger** A short knife, made for the purpose of stabbing rather than cutting.
- DAIRS** DIA Advanced Imagery Reproduction System.
- DARPA** Defense Advanced Research Projects Agency.
- DARTS** Design and Analysis of Reference Threat Signature.
- DASC** Deportable Alien Control System.
- Data mining** Statistical analysis techniques used to search through large amounts of data to discover trends or patterns.
- DAWS** Defense Automated Warning System.
- DBS** Direct Broadcast Satellite.
- dBW** The ratio of the power to one Watt in decibels.
- DC power** Direct current power.
- DCI** Director of the Central Intelligence Agency.
- DCIIS** Defense Counterintelligence Integrated Information System.
- DCP** Data Collection Platform.
- DCS** Defense Communications System.
- DDN** Defense Data Network.
- DDS** Defense Dissemination System.
- DE** DDS Dissemination Element.
- DEA** Drug Enforcement Administration.
- Dead drop** A prearranged spot at which one party passes information to another without actually meeting; or, the act of making such a transfer, as in “making a dead drop.” Often a dead drop also involves the transfer of money, as when a double agent leaves information for a handler, and the handler returns the favor with a cash payment.
- Dead-drop spike** A device, resembling a large, fat pencil, used for making dead drops. The blunt end has a cap that can unscrew, so that materials can be inserted into the air- and watertight chamber, while the pointed end makes it easy to hide the spike in the ground.
- Dead-letter box** A covert location where messages or other items are deposited for retrieval by other intelligence operatives. Also called a dead drop, they are most often used as a means of transferring documents and messages, but can also be used to funnel equipment and money to agents in the field.
- Debriefing** The process of interrogation, often planned and voluntary, designed to elicit information after a specific mission, event, or term of service.
- Declassification** The removal of restrictions on access to information. In some cases, declassification of a document is automatic after a certain period of time; in others, security considerations dictate a continuation of the classified status.
- Decontamination** The efforts to safeguard property and people that have been exposed to chemical, nuclear, or biological agents.
- Decryption** The reverse of encryption, the process by which ordinary data, or plain text, is converted into a cipher. To decipher a message requires a key, an algorithm that provides the method by which the message was encrypted.
- Deep cover** An agent who operates under many layers of legends or false backgrounds.
- Defector** A spy who voluntarily changes sides or leaves service to aid an “enemy” country or organization.
- Defector-in-place** Any agent who defects to the opposing side but who remains in his prior position with the intent to act as a double agent.
- DELTA force** Elite counter-terrorism group of the U.S. Army’s 1st Special Forces Operational Detachment-Delta.
- DES** Digital Encryption Standard. In the late 1970s, the U.S. government defined a cipher algorithm for standard use by all government departments, available also to the public. This early algorithm, the Digital Encryption Standard, is today in the process of being replaced by a new algorithm, the Advanced Encryption Standard.
- Descent (or terminal) phase** The final part of a ballistic weapon’s flight path, during which the warhead falls through the atmosphere toward its target.
- DEST** Domestic Emergency Support Team.
- Detonator** A device that activates an explosion by subjecting a charge of explosive to a high-pressure shock wave.
- DHKP** Revolutionary People’s Liberation Party/Front (DHKP/C).
- DI** Domestic Intelligence.
- DIA** Defense Intelligence Agency.

- Dial tone decoder** Telephone conversations are sometimes surreptitiously taped using microphones or other bugging devices. These devices run the risk of being detected. In some intelligence-gathering tapings, however, the contact telephone number may yield information that is as valuable as the actual conversation. If the content of a conversation is not essential, the contact telephone number can be obtained with a device called a dial tone recorder.
- Dictionary** In cyber intelligence: A computer programmed to scan intelligence data for specific terms and keywords.
- DIEPS** Digital Imagery Exploitation and Production System.
- Digital stenography** The hiding of message data in a digital medium.
- Digital watermarking** Information indicating ownership or embedded in a digital file.
- Diplomatic cover** Any agent secretly working for the diplomatic corps of a foreign country.
- Direction finder** An electronic device—typically a radio of some kind—used to locate a source of electronic emissions such as a ship or aircraft.
- Dirty bomb** A conventional bomb usually packed with low-level radioactive debris that can be spread over a wide area when the explosive detonates.
- Dirty tricks** Clandestine activities carried out by a covert-action group to discredit, destabilize, or eliminate an opposing regime, one of its agencies or departments, or an individual. A type of covert operation, dirty tricks include everything from the spreading of false rumors to sabotage, overthrow, and assassination.
- Disinformation** Secret information altered or provided in such a way as to make that information appear to be genuine.
- DISN** Defense Information Systems Network.
- DITDS** Defense Intelligence Threat Data System.
- DL/ID** Driver's license and identification.
- DMFE** Defense Automated Warning System Message Front End.
- DMS** Defense Message System.
- DNA** Deoxyribonucleic acid. The molecular composition of genetic material that is, in part, made up of nitrogenous bases that form a genetic code.
- DNA fingerprinting** The term applied to a range of techniques that are used to show similarities and dissimilarities between the DNA present in different individuals.
- DNA profile** Evaluation of an individual's DNA to establish a unique pattern of markers that can be used for identification purposes.
- DoD** United States Department of Defense.
- DODIIMS** DoD Intelligence Management System.
- DOE** United States Department of Energy.
- Domestic intelligence** Efforts by a government to obtain information about activities that pose an actual or putative threat to internal security.
- Doo transmitter** A radio transmission device camouflaged as a pile of animal droppings or, in its most common form, a large single fecal dropping from an animal indigenous to the area of intended use.
- Doppler radar** Radar that detects the frequency shifts in echoes from moving reflectors, and so can determine speed as well as range of a target.
- Double agent** Someone who seems to serve one intelligence agency, but actually works on behalf of another.
- Downlink** A satellite to Earth connection or electronic signal path.
- DPO** Domestic Preparedness Office.
- Drop** Intelligence parlance for the location at which an agent passes information to another, or the act of passing that information—as in “making a drop.”
- DS** United States Bureau of Diplomatic Security.
- DS&T** CIA Directorate of Science and Technology.
- DSB** Defense Science Board.
- DSNET** Defense Secure Network.
- DSS** Defense Security Service.
- DTIC** Defense Technical Information Center.
- Dual use technology** Tools or techniques, developed originally for military or related purposes, which are commercially viable enough to support adaptation and production for industrial or consumer uses.
- Dynamic address** A temporary Internet protocol (IP) address, assigned to a computer only during the time it is connected to the Internet.
- EA** Electronic Attack.
- E-beam** An irradiation method that can be used to decontaminate mail.
- Ebola virus** The species of Ebola virus are among a number of viruses that cause a disease, hemorrhagic fever, that is typified by copious internal bleeding and bleeding from various orifices of the body, including the eyes. The disease can result in death in over 90 percent of cases.
- E-bomb** An e-bomb, or electronic bomb, is a non-explosive artillery shell or missile that sends out an electromagnetic pulse (EMP) of enormous power, capable of permanently disabling mechanical and electronic systems.
- ECCM** Electronic Counter Counter Measures.
- Echelon** The name for a global surveillance network consisting of ground stations, satellites, and other listening posts, which collectively intercept and analyze worldwide electronic communications.
- ECM** Electronic Counter Measures.
- Economic espionage** Spying conducted for the benefit of a commercial or industrial enterprise, typically to gain information not available through open channels. Sometimes known as industrial espionage.
- Edge weapons** Knives and other devices with a sharp edge that can be used for murder or self-defense.
- EEG** Electroencephalogram.
- EES** Escrowed Encryption Standard program.

- EIRP** Effective Isotropic Radiated Power (a measurement of signal strength).
- EIS** Enhanced Imagery System.
- EKMS** Electronic Key Management System [NSA COMSEC].
- ELA** Revolutionary People's Struggle (ELA).
- Electromagnetic pulse (EMP)** Any nuclear explosion 25 miles (40 km) or higher above the ground produces a high-altitude electromagnetic pulse (HEMP), a short-lived, overlapping series of intense radio waves that blanket a large swath of ground. These radio waves can induce electrical currents in metallic objects and so cause damage to electrical and electronic equipment, including electrical power grids, telephone networks, radios, and computers.
- Electromagnetic spectrum** The complete range of electromagnetic waves on a continuous distribution from a very low range of frequencies and energy levels, with a correspondingly long wavelength, to a very high range of frequencies and energy levels, with a correspondingly short wavelength. Radio waves, visible light, and x rays are examples of electromagnetic waves at different frequencies. Every part of the electromagnetic spectrum is exploited for some form of military, security, or espionage activity; the entire spectrum is also key to science and industry.
- Electronic countermeasures (ECM)** An ECM, also known as an electronic attack, is a component of electronic warfare (EW), the use or control of electromagnetic energy either in defense, or for the purposes of a military attack on an enemy. Its counterpart is electronic protection or electronic counter-countermeasures (ECCM)—efforts or equipment directed toward the protection of persons or material from the effects of electronic warfare.
- Electronic warfare (EW)** The use or control of electromagnetic energy either in defense, or for the purposes of a military attack on an enemy. There are three components of electronic warfare: electronic countermeasures or electronic attack, electronic counter-countermeasures or electronic protection, and electronic warfare support.
- Electro-optical intelligence** The acquisition of data from the portion of the electromagnetic spectrum of wavelengths that contains ultraviolet radiation, visible light, and infrared radiation.
- ELINT** Electronics intelligence, or intelligence derived from the interception of non-communication electromagnetic signals, most notably radar. Subsets of ELINT include FISINT, or foreign instrumentation signals intelligence, and TELINT, or telemetry intelligence. ELINT is in turn a subset of signals intelligence (SIGINT).
- ELISA** Enzyme-linked immunoadsorbent assay.
- ELN** National Liberation Army (ELN)-Colombia.
- EM** Electromagnetic.
- EML** Environmental Measurements Laboratory.
- EMP** Electromagnetic pulse—an energy surge from a mechanical, electrical, chemical, or nuclear system, which can be used as a weapon.
- Encryption** The conversion of a message from plain text into cipher or code.
- Encryption of data** Data is any useful information and encryption is any form of coding, ciphering, or secret writing. Encryption of data, therefore, includes any and all attempts to conceal, scramble, encode, or encipher any information.
- Energy directed weapons** Weapons that use energy to disable or destroy equipment or people are referred to as energy directed weapons. Examples include lasers, high-power microwave weapons, and charged particle beam weapons.
- Energy harvesting** The gathering of energy from ambient sources, including sunlight, wind, wave action, water currents, geothermal components such as volcanoes, chemical and thermal gradients, barometric fluctuations, electromagnetic radiation, and human and other biological systems.
- ENIAC** American Electronic Numerical Integrator and Computer.
- Enigma** A ciphering (code communication) system used by the German military from 1926 until the end of World War II, and by several other nations for some years after. Enigma was the first mechanized message-encryption system to see wide use.
- Enrollment** The initial collection of the biometric data for setting up templates.
- Environmental security (DEM)** Aspects of national security that are driven by or that address environmental issues, either domestically or globally.
- Enzyme** A type of protein that affects the rate of chemical reactions in the body.
- EO** United States presidential executive orders.
- EOL** As a technical abbreviation, most commonly used to denote "End of Life" the point at which a system becomes inoperational.
- EPA** Environmental Protection Agency.
- EPCRA** Emergency Planning and Community Right-to-Know Act, legislation passed by Congress in 1986 to help communities respond to chemical hazards.
- EPDS** Electronic Processing & Dissemination System.
- Epitaxy** The growth of crystalline layers of semiconducting materials in a layered structure.
- EPR** Directorate of Emergency Preparedness and Response, Department of Homeland Security.
- Espionage** The use of spies, or the practice of spying, for the purpose of obtaining information about the plans, activities, capabilities, or resources of a competitor or enemy. It is closely related to intelligence, but is often distinguished from it by virtue of the clandestine, aggressive, and dangerous nature of activities.
- ETA** Basque Fatherland and Liberty (ETA).
- ETEP** Emanated transient electromagnetic pulses.
- Etiological** Involving disease and the causes thereof.
- EU** European Union.
- EURATOM** European Atomic Energy Community.
- EW** Electronic warfare and techniques that utilize and exploit properties of the electromagnetic spectrum.

- Executive order** A guideline issued by the President of the United States, directed toward a particular issue, and possessing the status of a de facto law. Unlike presidential directives, executive orders are unclassified.
- Executive Order 12863** Regarding: President's Foreign Intelligence Advisory Board.
- Executive Order 12958** Regarding: Classified National Security Information.
- Executive Order 12968** Regarding: Access to Classified Information.
- Executive Order 12977** Regarding: Interagency Security Committee.
- Executive Order 13224** Regarding: Freezing of terrorist organization assets.
- Exhaustion** Searching for a key or other secret quantity in code breaking by systematically checking all possibilities.
- Exposure dose** The quantity of a chemical that an organism receives from the environment through inhalation, ingestion, and/or contact with the skin.
- Extradite** To surrender an alleged criminal to another U.S. state or nation that has jurisdiction.
- FAA** United States Federal Aviation Administration.
- Facility security** The protection, and the measures taken toward the protection of a building or other physical location.
- FAISS** FORSCOM Automated Intelligence Support System.
- FAM** Federal air marshal.
- FARC** Revolutionary Armed Forces of Colombia (FARC).
- Farm, The** The nickname for the training school for CIA recruits in Virginia.
- Fatwa** A legal opinion or ruling issued by an Islamic scholar.
- FBI** United States Federal Bureau of Investigation.
- FBIS** CIA, Foreign Broadcast Information Service.
- FCA** Future Communications Architecture.
- FCC** Federal Communications Commission.
- FDA** United States Food and Drug Administration.
- FDMA** Frequency Division Multiple Access.
- FDS** Fixed Distributed System.
- FEMA** Federal Emergency Management Agency.
- FEST** United States Foreign Emergency Support Team.
- FIA** Future Imagery Architecture.
- FIC** Fleet Intelligence Center, which provided operational intelligence for the U.S. Navy from the 1960s until absorption of the FICs into the National Military Joint Intelligence Center (NMJIC) in 1991.
- FINCEN** Financial Crimes Enforcement.
- Fingerprints** The patterns on the inside and the tips of fingers. The ridges of skin, also known as friction ridges, together with the valleys between them form unique patterns on the fingers. Fingerprint analysis is a biometric technique comparing scanned image of prints with a database of fingerprints.
- Firewall** A system to prevent unauthorized access of computer hardware or software to or from a private network.
- FISA** The Foreign Intelligence Surveillance Act, which was passed by the United States Congress in 1978.
- FISH** German *Geheimschreiber* cipher machine.
- FISINT** Foreign instrumentation signals intelligence. Examples of FISINT include signals sent by foreign entities when testing and deploying aerospace, surface, and sub-surface systems. FISINT is a subset of ELINT, or electronic intelligence.
- Fission** A process in which the nucleus of an atom splits, usually into two daughter nuclei, with the transformation of tremendous levels of nuclear energy into heat and light.
- FISTA** Flying Infrared Signature Technology Aircraft.
- Flame analysis** A form of atomic emission analysis. The colors produced by the flame test are compared to known standards, and then the presence of certain elements in the sample can be confirmed. The color of the flame and its spectrum (component colors) is unique for each element.
- FLETC** Federal Law Enforcement Training Center (previously part of the Department of Treasury). On March 1, 2003, agents were transferred to the Department of Homeland Security (DHS), directorate of Border and Transportation Security (BTS).
- Flight Data Recorders** Hardened mechanical devices, designed to survive a crash, that record measurements of an aircraft's performance, navigation and flight configuration.
- Foggy Bottom** Nickname for headquarters of the United States Department of State.
- FOIA** Freedom of Information Act. Sometimes known as the Freedom of Information-Privacy Acts, a term referring to 1967 (FOIA) and 1974 (Privacy Act) statutes and their amendments, which greatly restrict government agencies' authority to collect information on individuals, and to withhold that information.
- Footprint** A geographically related map of signal strengths.
- Force projection** The ability to project or move an aggregation of military personnel from the continental United States (or another theatre) in response to military requirements.
- Foreign Broadcast Information Service (FBIS)** The pre-eminent collector of open source information for the United States government; it collects, translates, and disseminates foreign open source material for U.S. government use. It started as the Foreign Broadcast Monitoring Service (FBMS).
- Foreign Intelligence Surveillance Act** Public Law 95-511, Foreign Intelligence Surveillance Act (FISA).
- Forensic geology** The use of geologic principles and techniques to establish facts or provide evidence used in a court of law. The gathering and interpretation of geologic data for intelligence, espionage, and national security purposes can fall under the second definition of forensic geology.
- Forensic science** A multidisciplinary subject used for examining crime scenes and gathering evidence to be used in prosecution of offenders in a court of law. Forensic science

- techniques are also used to examine compliance with international agreements regarding weapons of mass destruction.
- FORMMS** Foreign Materiel Management System.
- FORTEZZA** NSA Crypto component of MISSI [formerly Tessera].
- FPS** Federal Protective Service (previously part of the General Services Administration). On March 1, 2003, agents were transferred to the Department of Homeland Security (DHS), directorate of Border and Transportation Security (BTS).
- FRVT** Face Recognition Vendor Test.
- FSB** The Federal Security Service (a Russian intelligence organization formerly known as the FSK).
- FSK** The Federal Counterintelligence Service was a Russian intelligence organization that was later reorganized and renamed the FSB.
- Fuselage** The central portion of an aircraft, which usually holds passengers or cargo.
- Fusion** The process by which two light atomic nuclei combine to form one heavier atomic nucleus. As an example, a proton (the nucleus of a hydrogen atom) and a neutron will, under the proper circumstances, combine to form a deuteron (the nucleus of an atom of “heavy” hydrogen). In general, the mass of the heavier product nucleus is less than the total mass of the two lighter nuclei. Fusion is the initial driving process of nucleosynthesis.
- G-2** The intelligence staff of a unit in the U.S. Army. It is contrasted with G-1 (personnel), G-3 (operations), and G-4 (supply). In the navy, these sections have their counterparts, each with an *N*-designation, while at the level of the Joint Staff, the sections use the prefix *J*-.
- GA nerve agent** Tabun, O-ethyl N,N-dimethylphosphorodiamidate.
- GAO** United States General Accounting Office.
- Gas chromatograph-mass spectrography (GC/MS)** An instrument used to analyze the molecular and ionic composition of chemical compounds. GC/MS technology combines two widely used laboratory techniques: gas chromatography (GC), which separates and identifies compounds in complex mixtures, and mass spectrometry (MS), which determines the molecular weight and ionic components of individual compounds.
- GB nerve agent** Sarin; O-isopropyl methylphosphonofluoridate.
- GBCS** Ground-based common sensor.
- GBS** Global Broadcast Service.
- GCHQ** United Kingdom Government Communications Headquarters.
- GD nerve agent** Soman; O-pinacolyl methylphosphonofluoridate.
- Genes** Made up of DNA, a gene is found in the cell nucleus and carries in its sequence all the instructions for the development of an organism and all its traits.
- Genetic information** The total accumulation of known genetic data on all organisms. The term may also be applied to individuals or families, i.e., the total known genetic data for a given person or family group.
- Genetic testing** Any clinical or research assay that evaluates the genes, DNA sequence, or mutations in a specimen. This may include analysis of chromosomes, cells, enzymes, or molecular testing.
- GENIE** Genetic Imagery Exploitation.
- Genome** The entire DNA sequence containing an organism’s genes.
- GEO** Geostationary earth orbit.
- GEODSS** Ground-based electro-optical deep space surveillance.
- Geostationary orbit (GEO)** A circular orbit at 35,780 km above Earth’s equator that allows satellites to maintain a steady position relative to the terrain below as expressed in degrees meridian (i.e., east or west of the prime meridian).
- Geosynchronous** A satellite orbit that keeps the satellite at a fixed point relative to the rotating surface of the Earth.
- Gestapo** The *Geheime Staatspolizei*, or Gestapo, a German secret police force, was created in 1933 after Adolf Hitler became chancellor of Germany. The Gestapo was created to help solidify Nazi control by identifying and arresting anti-Nazi agents in Germany. The agency was restructured several times during its twelve-year history and was instrumental in perpetrating the Nazi deportation and destruction of European Jews during the Holocaust.
- GF nerve agent** Cyclosarin cyclohexyl methylphosphonofluoridate nerve agent.
- GIA** Armed Islamic Group (GIA).
- GIS** The common abbreviation for Geographic Information Systems, a powerful and widely used computer database and software program that allows scientists to link geographically referenced information related to any number of variables to a map of a geographical area.
- Global Positioning System (GPS)** A constellation of twenty-four navigational satellites orbiting Earth, launched and maintained by the U.S. military. GPS receivers can decode signals from the satellites to calculate location and exact time.
- Globalization** The integration of economies and markets worldwide.
- Go pills** Dexamphetamine pills used by soldiers to fight fatigue.
- GPALS** Global protection against limited strikes.
- GPS** Global positioning system.
- GPU** USSR State Political Directorate.
- GRAPO** First of October Antifascist Resistance Group.
- Great Game** In intelligence history, the “Great Game” described a complex rivalry—characterized by wars, assassinations, and espionage conspiracies—between Britain and Russia for control of Central Asia and the Near East.
- GRIS** Global Reconnaissance Information System.
- GRU** USSR Military Intelligence.
- GSA** General Services Administration.

- GSD** Graphical situation display.
- GSM encryption** GSM stands for either “group special mobile” or “general system for mobile communications,” a protocol or standard for digital cellular communications. GSM encryption is the means by which phone conversations on networks using GSM are scrambled, such that they cannot be descrambled and intercepted by others.
- GSPC** Salafist Group for Call and Combat.
- GSR** Ground surveillance radars.
- GSS** Israeli General Security Service.
- G/T** Unit of measurement for an antenna derived from the gain and noise temperature. Generally, the higher the G/T ratio the stronger the antenna.
- GTO** Geostationary transfer orbit. Generally used to refer to the temporary orbit of a geostationary satellite destined for GEO orbit.
- Guerilla warfare** In the modern era, guerilla warfare refers to armed resistance by paramilitary or irregular groups toward an occupying force. Guerilla warfare also describes a set of tactics employed by smaller forces against larger, better equipped, and better supplied forces.
- HAARP** ELF/VLF radio detection of underground structures.
- Habeas Corpus** U.S. constitutional right to avoid unlawful detention or imprisonment. Taken from the Latin phrase “You have the body.”
- Hacker** A person who gains illegal access to, and sometimes tampers with, computer systems and the information they contain.
- Hacktivism** The use of computer hacking in the service of political activism.
- HAHO** A high altitude-high opening parachute jump.
- HALO** A high altitude-low opening parachute jump.
- HAMAS** Islamic Resistance Movement (HAMAS).
- HAMMER** Hazardous materials management and emergency response.
- HANAA** Nucleic acid analyzer.
- Handler** A case officer who works on a one-on-one basis with an agent.
- Hardening** In a general sense, hardening is the process of securing a computer. More specifically, hardening is the removal or disabling of all components in a computer system that are not necessary to its principal function or functions.
- Hemorrhagic fevers and diseases** Hemorrhagic diseases are caused by infection with viruses or bacteria. As the name implies, a hallmark of a hemorrhagic disease is copious bleeding.
- Hertz (Hz)** Unit of frequency; 1 Hz equals one cycle per second.
- HEU** Highly-enriched uranium.
- HF-band** 1.8–30 MHz.
- HHS** Health and Human Services Department.
- High-power microwave (HPM) weaponry** High-power microwave weaponry sends out a short, extremely high-voltage burst of electromagnetic energy capable of disrupting computer systems for a fraction of a second.
- HIMS** Human information management system.
- HPSC** High Performance Scientific Computing Research System.
- HSMN** Homeland Security Monitoring Network.
- HT** A mixture of distilled mustard gas compound and Agent T.
- HUAC** U.S. House Un-American Activities Committee.
- HUJI** Harakat ul-Jihad-I-Islami.
- HUJI-B** Harakat ul-Jihad-I-Islami/Bangladesh.
- HUM** Harakat ul-Mujahidin (Movement of Holy Warriors).
- HUMINT** Human intelligence, the gathering of information through human contact. HUMINT is, along with signals intelligence and imagery intelligence (SIGINT and IMINT respectively), one of the three traditional means of intelligence-gathering.
- Hydrophone** An underwater microphone sensitive to acoustic disturbances.
- Hypersonic aircraft** A plane capable of flying at Mach 5, or five times the speed of sound. At sea-level atmospheric pressure, with air temperatures of 59°F (15°C), the speed of sound is about 760 miles per hour (1,225 k.p.h.).
- IAA** Islamic Army of Aden.
- IAEA** International Atomic Energy Agency.
- IAFIS** Integrated automated fingerprint identification system (FBI system).
- IAIP** Information Analysis and Infrastructure Protection, Department of Homeland Security.
- IAS** Intelligence Analysis System.
- IBIS** The Interagency Border Inspection System (IBIS) is a database of names and other identifying information used to deter and append suspects—including suspected terrorists—as they attempt to pass through international border crossing checkpoints.
- IBS** Integrated Broadcast Service.
- IC4I** Integration for Command, Control, Communications, Computers and Intelligence.
- ICARIS** Intelligence Communications and Requirements Information System.
- ICBM** Intercontinental ballistic missile.
- IDC** International Data Centre.
- IDENT** The Automated Biometric Identification System (IDENT) is a database system using automated fingerprint identification systems (AFIS) technology as part of programs supervised by the U.S. Department of Homeland Security that intend to thwart illegal entry into the United States by criminal aliens.
- Identification** In biometrics, a one-to-many comparison against the entire enrolled population.

- Identity theft** An identity thief typically obtains access to a victim's social security number, driver's license information, bank account numbers, credit card numbers, etc. with the intent to open accounts in the victim's name and make purchases or perform other transactions.
- IDHS** Intelligence data handling system.
- IESA** International Environmental Sample Archive.
- IFF** Identification friend or foe (IFF) systems are a means of identifying aircraft, ships, and vehicles using electronic means. Applied by both military and civilian entities, IFF—which in its civilian form is more properly known as the air traffic control radar beacon system, or ATRCBS—uses radar to identify aircraft, which are assigned unique identifier codes. There are various modes of operation for IFF, depending on the level of security desired.
- IFSARE** Interferometric synthetic aperture radar—elevation.
- IG** Al-Gama'a al-Islamiyya (Islamic Group, IG).
- Image intensification** Amplification of dim patterns of reflected light to make a visible image; used in night-vision scopes.
- IMETS** Integrated Meteorological System.
- IMF** International Monetary Fund.
- IMINT** Imagery intelligence, or intelligence derived from photography, infrared sensors, synthetic aperture radar, and by other forms of imaging technology. Once known as PHOTINT or photographic intelligence, IMINT is one of the four major branches of intelligence, along with HUMINT, MASINT, and SIGINT (human, measurement and signatures, and signals intelligence respectively).
- IMS** International Monitoring System.
- IMU** Islamic Movement of Uzbekistan.
- Inclined orbit** A satellite with a figure "8" like orbit that travels across Earth's equator.
- Indications and warnings (IW)** Intelligence that relates to time-sensitive information involving potential threats.
- INF** United States Bureau of Intelligence & Research.
- Infectious diseases** Diseases that are caused by microorganisms such as bacteria and viruses, many of which are spread from person to person. An intermittent host, or vector, aids the spread of some infectious diseases.
- Information security** Information security, often compressed to "infosec," is the preservation of secrecy and integrity in the storage and transmission of information.
- Information warfare** A general term encompassing a variety of tools and techniques, including psychological warfare, jamming of broadcasts, computer hacking, and cyberwarfare.
- Infrared detection devices** Sensors that detect radiation in the infrared portion of the electromagnetic spectrum ( $>10^{12}$  to  $5 \times 10^{14}$  Hz).
- Infrared imaging** Detection of infrared radiation emitted by objects in a scene followed by creation of a visible-light image.
- INL** International Narcotics and Law Enforcement Affairs, United States Bureau for.
- INM** Bureau of International Narcotics Matters.
- INS** As of March 1, 2003, the newly created United States Department of Homeland Security (DHS) absorbed the former Immigration and Naturalization Service (INS). All INS border patrol agents and investigators—along with agents from the U.S. Customs Service and Transportation Security Administration—were placed under the direction of the DHS Directorate of Border and Transportation Security (BTS). Responsibility for U.S. border security and the enforcement of immigration laws was transferred to BTS. Former INS immigration service functions are scheduled to be placed under the direction of the DHS Bureau of Citizenship and Immigration Services. Under the DHS reorganization plan, the INS formally ceases to exist on the date the last of its functions are transferred.
- INSC** International Nuclear Safety Center.
- INSCOM** U.S. Army Intelligence and Security Command.
- INSPASS** Immigration and Naturalization Service Passenger Accelerated Service System.
- Integrated circuits** Complex electronic circuits fabricated using multiple growth and lithography/pattern transfer stages to produce many miniature electronic elements on a monolithic device.
- Intelligence** Information concerning a foreign entity, usually (although not always) an adversary, as well as agencies concerned with collection of such information. It is intimately tied with the intelligence cycle, a process whereby raw information is acquired, converted into intelligence, and disseminated to the appropriate consumers.
- Intelligence agent** In general terms, an agent is one authorized to act in place of, or on behalf of, another. An intelligence agent, however, is not simply an agent of or for an intelligence agency. Whereas members of the agency are called intelligence officers, operatives, or special agents, an agent is someone hired or recruited from outside. There are numerous other variations in the informal taxonomy of agents, including secret or undercover agents, agents provocateur, agents-in-place, double agents, etc.
- Intelligence Authorization Act** The 1981 congressional act that established the process whereby the CIA notifies the leadership of the House and Senate Intelligence Committees of covert actions.
- Intelligence officer** A professional employed by an intelligence service. Members of the intelligence community make sharp distinctions between intelligence officers and intelligence agents, who are outsiders employed by the intelligence agency. Intelligence officers, on the other hand, are operatives of the agency itself, but their professional role—and the fact that many are military officers and/or intelligence specialists—gives them particular distinction.
- Intercept** Intelligence gathered through electronic eavesdropping.
- Internet** A vast worldwide conglomeration of linked computer networks. The most significant component of the Internet is the World Wide Web.
- Internet dynamic and static addresses** Every computer operating on the Internet has a unique IP, or Internet protocol, address. Because the Internet's original design did not take into account the vast size it would assume from the mid-1990s onward, as more and more people went online, the architecture did not account for an infinite number of IP

- addresses. To conserve these, an Internet service provider (ISP) has a limited number of permanent IP addresses, and issues temporary IP addresses for customers to use while online.
- Internet Spider** A program designed to “crawl” over the World Wide Web, the portion of the Internet most familiar to general users, and retrieve locations of, and information from Web pages.
- Internet surveillance** The monitoring of Internet data traffic for information useful to government authorities.
- Internet tracking and tracing** Electronic passage through the Internet leaves a trail that can be traced. Tracing is a process that follows the Internet activity backwards, from the recipient to the user.
- INTERPOL** International Criminal Police Organization.
- Interrogation** A conversational process of information gathering. The intent of interrogation is to control an individual so that he or she will either willingly supply the requested information or, if someone is an unwilling participant in the process, to make the person submit to the demands for information. The latter can involve techniques of humiliation, intimidation, and fear. In more extreme cases, in some countries, physical pain is inflicted.
- Intifada** Literally, “shaking off,” a term applied to the Palestinian uprising against Israel’s occupation of the West Bank and Gaza.
- IOL** Inter-orbit link.
- IOM** Institute of Medicine.
- IOSA** Integrated Overhead SIGINT Architecture.
- IPDS** Imagery Processing & Dissemination System.
- IPL** Imagery Product Library.
- IRA** Irish Republican Army.
- Irradiation** Using radiation, primarily for sanitization purposes, such as in use for irradiating mail by the United States Postal Service.
- IRS** Internal Revenue Service.
- ISAR** Inverse Synthetic Aperture Radar.
- ISFAR** Interferometric Synthetic Aperture Radar.
- ISMC** Intel Link Systems Management Center.
- ISMS** Integrated Security Management System.
- Isotope** A form of a chemical element distinguished by the number of neutrons in its nucleus. E.g., <sup>233</sup>U and <sup>235</sup>U are two isotopes of uranium; both have 92 protons, but <sup>233</sup>U has 141 neutrons and <sup>235</sup>U has 143 neutrons.
- IT** Information technology, a term that encompasses computers and related materials, machines, and processes.
- IUSS** Integrated Undersea Surveillance System.
- IW** Indications and warnings. Intelligence that relates to time-sensitive information involving potential threats.
- J-2** Joint intelligence, the office supporting the intelligence needs of a joint or unified command. For the Joint Chiefs of Staff, the Defense Intelligence Agency serves the J-2 function.
- Jamming** Blocking of electronic signals.
- JDAM** Joint Direct Attack Monition (JDAM) is a satellite-guided “smart” bomb capable of accurate and high precision strikes in any weather.
- JDISS** Joint Deployable Intelligence Support System.
- JEM** Jaish-e-Mohammed (Army of Mohammed).
- Ji** Jemaah Islamiya.
- JIC** Joint intelligence center, or the intelligence center of a command headquarters. For the Joint Chiefs of Staff, the National Military Joint Intelligence Center serves this function.
- Jihad** In Islam: A holy struggle or war.
- JIRONET** Joint Intelligence Research Office Network.
- JMIP** The Joint Military Intelligence Program, an annual budget request for military intelligence presented by the Secretary of Defense to the President of the United States.
- JN-25** Japanese Navy-25, the name given to the Japanese military operational code during World War II.
- JRA** Japanese Red Army.
- JSTARS** Joint Surveillance Target Attack Radar System.
- JSTARS-CGS** JSTARS Common Ground Station.
- JSTARS-GSM** JSTARS Ground Station Module.
- JTT** Joint Tactical Terminal.
- JUI-F** Jamiat Ulema-I-Islam Fazlur Rehman faction.
- JWICS** Joint Worldwide Intelligence Communications System.
- Ka-band** Generally between 18 to 31 GHz.
- Key** An algorithm that provides the method by which a message was encrypted.
- Keyhole** Since 1962, code name for US photoreconnaissance satellites.
- KGB** USSR *Komitet Gosudarstvennoi Bezopasnosti* (Committee of State Security). The USSR equivalent of the American CIA.
- KH** Cameras, KH series.
- Kiloton** A measure of energy used to quantify the size of large explosions, especially nuclear explosions. One kiloton is equivalent to the energy produced by the explosion of 1000 tons of TNT.
- KMM** Kumpulan Mujahidin Malaysia.
- LANL** Los Alamos National Laboratory.
- L-band** 1.530–2.700 GHz.
- LBNL** Lawrence Berkeley National Laboratory.
- LC50** The chemical concentration required to kill 50 percent of test subjects.
- LCLO** The minimal chemical concentration found to be lethal.
- LD50** Lethal dose for 50 percent of those exposed to a toxic agent.
- LDLO** The minimal dose strength found to be lethal.



**L-Gel decontamination reagent** A coating that was developed at Lawrence Livermore National Laboratory (LLNL) in Berkeley, California. The coating is effective at decontaminating areas exposed to both chemical and biological agents.

**Legend** A false background or biography.

**LEO** Low earth orbit.

**LEPC** Local Emergency Planning Committee.

**Less lethal weapons** Tools and techniques designed for riot control and other security functions with the intention of neutralizing hostile activity without killing or causing permanent bodily harm.

**Lewisite blistering agent** Chlorovinyldichloroarsine.

**Light detection and ranging (LIDAR)** An active remote sensing system that allows exceptionally accurate and rapid determination of terrain and structural features (e.g. height). LIDAR produces highly accurate three dimensional data measurements that can then be utilized by mapping, guidance, and navigation systems.

**LLNL** Lawrence Livermore National Laboratory.

**LNA** Low-noise amplifier.

**LOCE** Linked Operations/Intelligence Centers Europe.

**Lock-picking** An ability to open locks without the key specific for the lock.

**Looking Glass** The nickname for the Airborne Command Post, a mission operated continuously by U.S. Strategic Air Command (SAC) between 1961 and 1990. For almost three decades, SAC had an aircraft aloft 24 hours a day, seven days a week.

**Lord Haw-Haw** The nickname of Nazi propagandist and broadcaster, William Joyce. During World War II, Joyce broadcast a well-known English-language propaganda show from Berlin, often taunting Allied forces. Though never calling himself Lord Haw-Haw on air, he became infamous among Allied combat troops and British citizens.

**LRA** Lord's Resistance Army.

**LT** Lashkar-e-Tayyiba (Army of the Righteous).

**LTBT** Limited (Nuclear) Test Ban Treaty.

**LTTE** Liberation Tigers of Tamil Eelam.

**LVF** Loyalist Volunteer Force.

**Mach** The speed of sound in air (under certain temperature conditions) is called Mach 1. Mach 2 is twice that speed and so on.

**MAD** Mutually assured destruction (Cold War security and defense policy).

**MAE UAV** Predator medium altitude endurance unmanned aerial vehicle.

**Magic** The codename given to the U.S. Navy Combat Intelligence Unit's effort to break the JN-25 Japanese code during World War II.

**Magic chips** Micro array of gel-immobilized compounds.

**MAGIS** Marine Air-Ground Intelligence System.

**Magnitude** The size of an earthquake, typically reported using the Richter scale. As originally defined by Richter, the

magnitude of an earthquake is the logarithm of the amplitude of the largest seismic wave recorded on a particular kind of seismometer located 100 km from the earthquake epicenter. Seismologists today use a variety of magnitude scales that produce similar, but not identical, estimates of earthquake size.

**Mail sanitization** The process in which mail is decontaminated. The process of mail sanitization can be applied as a precautionary measure to kill micro-organisms that may be contained in the mail or to sterilize mail that is known to be contaminated with dangerous microorganisms.

**MALDI-MS** Matrix-assisted laser desorption/ionization mass spectrometry.

**Malicious data** Data that, when introduced to a computer—usually by an operator unaware that he or she is doing so—will cause the computer to perform actions undesirable to the computer's owner. It often takes the form of input to a computer application such as a word-processing or data spreadsheet program. It is thus, distinguished from a malicious program such as a computer virus, compared to which malicious data is perhaps even more stealthy.

**Manhattan Project** The Manhattan Project (officially the Manhattan Engineer District) was a secret, World War II effort by the United States to design and build the world's first nuclear weapon. Commanding the efforts of the world's greatest physicists and mathematicians during World War II, the \$20 billion project resulted in the production of the first uranium and plutonium bombs. The American quest for nuclear explosives was driven by the fear that Hitler's Germany would invent them first and thereby gain a decisive military advantage.

**Mapping Technology** A broad term that describes the equipment and techniques used to prepare, analyze, and distribute maps of all kinds.

**Marshall Plan** American economic aid program designed to facilitate the reconstruction of Western Europe after World War II.

**MARV** Miniature autonomous robotic vehicle.

**MASINT** Measurement and signature intelligence. The term refers to forms of information gathered by means other than through the traditional ones, which include analysis of signals (SIGINT), imagery (IMINT), or data acquired through human contact (HUMINT). MASINT includes acoustic intelligence (ACINT), infrared intelligence (IRINT), laser intelligence (LASINT), nuclear intelligence (NUCINT), optical intelligence (OPINT), and unintentional radiation intelligence (RINT).

**Mass spectrometry** Separation of ions in a magnetic field according to their masses.

**MAV** Micro-air vehicle.

**MAXI** Modular Architecture for eXchange of Intelligence.

**McCarthyism** Period of anti-communist fervor in American politics in late 1940s and early 1950s; taken from the name of its chief proponent, U.S. Senator Joseph McCarthy of Wisconsin.

**MCGPS** Mapping, Chart, and Graphics Production System.

**MCI** United States Marine Corps Intelligence.

- Measurement and signatures intelligence (MASINT)** Information gathered by analysis of signals (SIGINT), imagery (IMINT), or data acquired through human contact (HUMINT).
- MEK** Mujahedin-e Khalq Organization (MEK of MKO).
- Meltdown** A nuclear power plant accident in which the molten uranium of the ruined core will coalesce into a single superheated mass and melt its way down to the groundwater below the plant, causing a violent steam explosion and dispersing even larger quantities of radioactive material. Also known as the China Syndrome.
- MEMS** Microelectromechanical systems.
- MERIT** Military exploitation of reconnaissance and intelligence technology.
- MGB** USSR Ministry of State Security.
- MI5 (British Security Service)** Best known by its designation as MI5, the Security Service is the leading counterespionage agency working in the United Kingdom. Its functions are somewhat akin to those of the United States Federal Bureau of Investigation, but MI5 places a much greater emphasis on intelligence, and its operatives have no arrest powers.
- MI6 (British Secret Intelligence Service)** Officially known as the Secret Intelligence Service (SIS), MI6 is the chief British foreign intelligence organization, analogous to the United States Central Intelligence Agency.
- MIC** Maritime Intelligence Center.
- Microchannel** In an light amplification device, a narrow cylinder of biased semiconductor that amplifies electron flow.
- Microchip** Microchips, also termed “integrated circuits” or “chips,” are small, thin rectangles of a crystalline semiconductor, usually silicon, that have been inlaid and overlaid with microscopically patterned substances so as to produce transistors and other electronic components on its surface.
- Microdot** A miniature photograph less than 1mm in diameter.
- Microfilm** Miniature films used for photographing objects and documents. The images on these films cannot be seen without an optical aid, either in a form of a magnifying glass or a projector.
- Microphones** A transducer converting the sound waves into electrical signals proportional to the strength of the sound. The microphone output can be recorded or transmitted.
- Microsat** Generally defined as a satellite weighing between 22.2 lbs to 222 lbs (10 to 100 kg).
- MIGS** Multi-Source Intelligence Ground System.
- MIIDS** Military Intelligence Integrated Data System.
- Minisat** Generally defined as a satellite weighing between 220 lbs to 2200 lbs (100 to 1000 kg).
- MINS** Multisource Integrated Notification System.
- MINT** Multi-Source Intelligence Tools.
- MKO** Mujahedin-e Khalq Organization.
- MMWR** CDC’s Morbidity and Mortality Weekly Report.
- MOAB** In addition to its raw destructive power, the Massive Ordnance Air Burst bomb (MOAB) has become part of a military and intelligence effort to discourage and demoralize enemy forces. Upon detonation, MOAB produces a mushroom cloud similar to a nuclear blast. The MOAB bomb is the most powerful non-nuclear weapon in the U.S. arsenal.
- Moderator** Substance that separates fuel elements in a nuclear reactor, slowing down neutrons to increase the likelihood that they will cause further fission events.
- Mole** An agent who has infiltrated an enemy’s intelligence organization.
- Money laundering** Hiding the profits earned from criminal activities by converting them into a different type of currency or asset, or by moving them to a secretive place.
- Mossad** Israeli Institute for Intelligence and Special Tasks.
- MP** Military police.
- MPAS** Measurement and signature intelligence analysis.
- MPC&A** Materials Protection, Control, and Accounting, NNSA.
- MRTA** Tupac Amaru Revolutionary Movement.
- MT** Machine translation.
- Multisensory grenades** Grenades emitting disorienting light flashes, painfully loud sounds, and possibly disagreeable odors.
- Multispectral** An adjective describing a sensor that is able to record signals in more than one band of electromagnetic wavelengths, or an image produced using such a sensor.
- MUSIC** Multi-User Special Intelligence Communications System [NAVSECGRU].
- Mustard gas** A substance used in chemical warfare. It is the popular name for the compound with the chemical designation 1,1-thiobis(2-chloroethane) (chemical formula: Cl-CH<sub>2</sub>-CH<sub>2</sub>-S-CH<sub>2</sub>-CH<sub>2</sub>-Cl). Mustard gas has a number of other names by which it has been known over the years, including H, yprite, sulfur mustard and Kampstoff Lost.
- MW** Molecular weight.
- NACDF** National Area Coverage Data Files.
- NACIC** National Counter Intelligence Center.
- NAILS** The National Automated Immigration Lookout System (NAILS) is a centralized database and computing system used by entry inspectors to identify aliens not eligible for admission.
- NALU** National Army for the Liberation of Uganda.
- Nanosat** Generally defined as a satellite weighing between 2.2 lbs. and 22 lbs. (1 to 10 kg).
- Nanotechnology** Device components ranging in size between 1/10,000,000 (one ten millionth of a millimeter) and 1/10,000 millimeter.
- NAPP** National Aerial Photography Program.
- NARA** National Archives and Records Administration.
- NARAC** United States National Atmospheric Release Advisory Center.

- Narcoanalysis** A psychotherapeutic method which uses a sedative or hypnotic drug as an aid to compel patients to speak without inhibition.
- Narcoterrorism** Terrorism undertaken by groups directly or indirectly involved in producing, transporting, or distributing illegal drugs.
- NAS** National Academy of Science.
- NASA** National Aeronautics and Space Administration.
- National command authorities** Within a national government, the national command authorities are the persons or officeholders (or their duly deputized alternates or successors) who have the legal power to direct military activities.
- National Intelligence Estimate(NIEs)** Reports by the National Intelligence Council (NIC), drawing on estimative views from across the Intelligence Community.
- NATO** North Atlantic Treaty Organization.
- NCA** National Command Authority.
- NCIC** National Crime Information Center.
- NCIS** Navy Criminal Investigative Service.
- NCIX** National Counterintelligence Center (NACIC), the U.S. Office of the National Counterintelligence Executive (NCIX) was created early in the twenty-first century. It educates members of government organizations and the private sector on the need to maintain vigilance against espionage, both political/national and economic/industrial. NCIX conducts regional seminars, issues publications, and produces other materials.
- NCLIS** United States National Commission on Libraries and Information Science.
- NCR** National Council of Resistance.
- NCS** National Communications System.
- NDIC** Department of Justice National Drug Intelligence Center.
- NDPO** Domestic Preparedness Office, United States National.
- NDTA** National Drug Threat Assessment.
- Need to know** A demonstrable and recognized purpose for accessing specific information.
- NERSC** National Energy Research Scientific Computing Center.
- Nerve gas** Nerve gases, or nerve agents, are mostly odorless compounds belonging to the organophosphate family of chemicals that inhibit the enzyme acetylcholinesterase and disrupt the transmission of nerve impulses in the body.
- NES** NIMA/National Exploitation System.
- NEST team** Nuclear Emergency Support Team.
- Network** A group of computers linked by communication lines.
- Network** A group of individuals or cells (subgroups) engaged in specific operations (e.g., espionage or terrorist operations).
- Neurotransmitter** A chemical that functions to pass a nervous impulse chemically through the synapse (gap) separating neurons (nerve cells).
- NFIB** The National Foreign Intelligence Board (NFIB) was created by the National Security Act of 1947. The NFIB acts as a communications channel among various national intelligence agencies and facilitates interagency exchange of information. The board also develops policy regarding the protection of intelligence information.
- NFIP** The National Foreign Intelligence Program, an annual budget request for the Intelligence Community, presented to the President of the United States by the Director of Central Intelligence.
- NGP** Non-governmental organization.
- NHAP** National High Altitude Photography Program.
- NI** Naval Intelligence.
- NIC** National Intelligence Council.
- NIF** National Ignition Facility.
- Night scopes** Infra-red scopes. Night vision scopes are devices that enable machines or people to “see in the dark,” that is, to form images when illumination in the visible band of the electromagnetic spectrum is inadequate.
- NIH** National Institutes of Health.
- NIJ** National Institute of Justice.
- NIM** United Kingdom National Intelligence Machinery.
- NIMA** National Imagery and Mapping Agency.
- NIPC** National Infrastructure Protection Center.
- NIPR** Revolutionary Proletarian Initiative Nuclei.
- NIPRNET** Non-Classified Internet Protocol Router Network.
- NIS** Navy Criminal Investigative Service.
- NISAC** National Infrastructure Simulation and Analysis Center.
- NIST** The National Institute of Standards and Technology (NIST) is a non-regulatory federal agency under the aegis of the Undersecretary for Technology in the U.S. Department of Commerce. It is concerned with maintaining measurement and calibration standards, including those related to a number of Homeland Security projects and agencies.
- NITFS** National Imagery Transmission Format.
- NIWA** Naval Information Warfare Activity.
- NKVD** USSR People’s Commissariat of Internal Affairs.
- NLA** The National Liberation Army of Iran.
- NMD** National Missile Defense.
- NMIC** The National Maritime Intelligence Center (NMIC) brings together intelligence operations for the United States: Navy, Marine Corps, and Coast Guard.
- NMJIC** United States National Military Joint Intelligence Center.
- NMR** Nuclear magnetic resonance.
- NNSA** National Nuclear Security Administration.
- Nonpersistent chemical warfare agent** Chemical warfare agents that maintain toxicity for a brief time (or until dispersed by weather).

- NORAD** The North American Air Defense Agreement, signed on May 12, 1958, by the United States and Canada, created a continental air defense warning and surveillance system in response to Cold War fears of an airborne attack by the Soviet Union. The resulting North American Air/Aerospace Defense Command (NORAD) has since shifted strategies from guarding against long-range bombers to warning of ballistic missile attacks and maintaining space surveillance.
- NPA** New People's Army.
- NPIC** National Photographic Interpretation Center.
- NPT** Non-Proliferation Treaty (nuclear weapons).
- NQR** Nuclear quadrupole resonance.
- NRC** Nuclear Regulatory Commission.
- NRIS** National Radar Imagery Interpretation Standard.
- NRO** National Reconnaissance Office.
- NRT** National Response Team.
- NRTD** Near real time dissemination.
- NS/EP** National security and emergency preparedness.
- NSA** The National Security Agency (NSA) is the leading cryptologic organization in the United States intelligence community. Focused on cryptologic and cryptanalytic missions, it is the nation's leading employer of mathematicians.
- NSC** National Security Council, the U.S. president's Intelligence Advisory Council.
- NSD** National Signal Databases.
- NSF** National Science Foundation.
- NSOC** National SIGINT Operations Center.
- NTA** Anti-Imperialist Territorial Nuclei.
- NTSB** National Transportation Safety Board.
- NTTC** National Technology Transfer Center (Emergency Response Technology Program).
- Nuclear Emergency Support Team (NEST)** An emergency response asset of the National Nuclear Security Administration (NNSA).
- Nuclear reactors** Complex devices in which fissionable elements such as uranium, thorium, or plutonium are made to undergo a sustainable nuclear chain reaction. This chain reaction releases energy in the form of radiation that (a) sustains the chain reaction; (b) transmutes (i.e., alters the nuclear characteristics of) nearby atoms, including the nuclear fuel itself; and (c) may be harvested as heat.
- Nuclear spectroscopy** A powerful tool in the arsenal of scientists and forensic investigators because it allows detailed study of the structure of matter based upon the reactions that take place in excited atomic nuclei.
- Nuclear weapons** Explosive devices that utilize the processes of fission and fusion to release nuclear energy.
- Nucleic acid analyzer (HANAA)** HANAA is an acronym for the hand-held advanced nucleic acid analyzer. HANAA is a real time polymerase chain reaction (PCR) based system for detecting pathogens (disease-causing organisms).
- Nuclide** A type of atom having a specific number of protons and neutrons in its nucleus.
- OAR** Office of Air and Radiation.
- OARS** Outlying Area Reporting Station.
- OASIS** Over-the-Horizon (OTH) Airborne Sensor Information System (OASIS).
- Observable** Any form of energy radiated by an object, such as an aircraft, that might be observed by an opponent.
- OEM** Office of Emergency Management.
- OER** Office of Emergency Response, United States Department of Energy (DOE).
- OERR** Office of Emergency and Remedial Response. An administrative office of the Environmental Protection Agency (EPA) in charge of administering the Superfund Program and initial responses to environmental crises.
- OFAC** United States Office of Foreign Asset Control.
- Official Secrets Act, United Kingdom** The Official Secrets Act of the United Kingdom prohibits the transfer of information deemed sensitive to national security interests.
- OGC** United States Offices of Global Communications.
- OGPU** USSR Unified State Political Directorate.
- OIG** United States Office of the Inspector General.
- OILSTOCK** NSA Geographic Information System.
- OIPR** United States Office of Intelligence Policy and Review.
- OIS** United States Office of Information Security.
- OIW** Ops/Intel Workstation.
- Oligonucleotide** A chemically synthesized short single-stranded DNA molecule.
- One-time pad** A cipher pad intended to be used for the encipherment and decipherment of a single message.
- ONI** Office of Naval Intelligence.
- ONR** Office of Naval Research.
- OPEC** Organization of Petroleum Exporting Countries, a cartel controlling much of the world's petroleum production.
- Open code** Communicating openly, but with the use of references with significant meaning to the recipient.
- Open sources** Non-classified sources that include such sources as official statistical publications, newspapers, radio broadcasts, and trade publications.
- Operational intelligence** Intelligence involved in military planning for a particular theatre or area of operations.
- Operative** An employee of an intelligence agency. Compare with *agent* and *intelligence officer*.
- ORNL** Oak Ridge National Laboratory.
- OSIS** Open Source Information System.
- OSIS** Ocean Surveillance Information System.
- OSS** Office of Strategic Services, forerunner of the CIA.
- OV** Orange Volunteers.

- Overflight** A mission by a spy plane over an enemy country to collect intelligence using electronic or photographic equipment.
- Overt information** Information gathered from published sources.
- P-3** P-3 Orion anti-submarine maritime reconnaissance aircraft.
- PAGAD** People Against Gangersterism and Drugs.
- PAM** Payload assist module.
- Parabolic microphone** A microphone inside a dish, able to pick up sounds from a distance.
- Parallel processing** The use of two or more computers working in tandem to solve a problem.
- Paroles** Key words or signals used to establish mutual identification.
- PARSEC** SIGINT Analysis and Reporting software.
- Passive SONAR** A sensitive listening-only SONAR mode to detect presence of objects making noise.
- Pathogen Genomic Sequencing** The Pathogen Genomic Sequencing program focuses on characterizing the genetic components of pathogens in order to develop novel diagnostics, treatments and therapies for the diseases they cause.
- Pathogens** Organisms, frequently microorganisms, or components of these organisms, that cause disease. Many diseases caused by microbial pathogens, and the frequency of these diseases, are a national security issue.
- Patriot act** The Patriot Act, or Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (Public Law 107–56), was signed into law on October 26, 2001, in the wake of terrorist attacks on the World Trade Center and Pentagon. The law grants law enforcement and intelligence agencies more power to detain and question suspects for longer periods of time, and increases their ability to conduct surveillance operations.
- Patriot missile system** An advanced ground-based air defense system.
- Payload** An object that is delivered by a missile or other rocket.
- P-band** 0.230–1.000 GHz.
- PCR** The polymerase chain reaction (PCR), refers to a widely used technique in molecular biology involving the amplification of specific sequences of genomic DNA, the genetic material found in virtually all living cells.
- Penetrability** The ease with which soil, rock, concrete, or other material can be penetrated by projectiles or other earth penetrating weapons.
- Penicillin** The first antibiotic. Discovered by Sir Alexander Fleming, it is produced by a species of a mold microorganism.
- Perigee** An orbital position where a satellite is closest to Earth.
- Persistent chemical warfare agent** Chemical warfare agents that maintain toxicity for a prolonged period (usually several days).
- PET** Positron emission tomography.
- PFIAB** The President’s Foreign Intelligence Advisory Board (PFIAB) provides unbiased monitoring of the overall intelligence effort of the United States by continually reviewing the activities of agencies and departments engaged in intelligence work.
- PFLP** Popular Front for the Liberation of Palestine.
- PFLP-GC** Popular Front for the Liberation of Palestine-General Command.
- PGP** Pretty Good Privacy, an encryption program.
- Photographic Interpretation Center** The Central Intelligence Agency (CIA) established the National Photographic Interpretation Center (NPIC) in the 1950s to provide skilled interpretation of photographic images obtained by low- and high-flying aircraft, and later by satellites. In 1973 the NPIC, originally a unit of the CIA Directorate of Intelligence, transferred to the Directorate of Science and Technology (DS&T). In 1996, it was moved to the newly formed National Imagery and Mapping Agency (NIMA).
- Photographic resolution** The term *resolution*, in the context of photography, refers to the degree to which adjacent objects can be distinguished from one another in a photographic image.
- PHS** Public Health Service.
- PIADC** Plum Island Animal Disease Center.
- PIC** Pressurized ionization chamber.
- Picosat** Generally defined as a satellite weighing less than 2.2 lbs (1 kg).
- PIDS** Perimeter Intrusion Detection System.
- PIJ** Palestine Islamic Jihad.
- PINES** Pacific Air Forces Interim National Exploitation System.
- PIRA** Provisional Irish Republican Army.
- PKK** Kurdistan Workers’ Party (PKK).
- Plaintext** A message in ordinary language that is to be enciphered.
- Playfair cipher** The Playfair cipher is a method of cryptography invented in 1854 by English physicist Sir Charles Wheatstone (1802–1875).
- PLF** Palestine Liberation Front.
- PLO** Palestine Liberation Organization.
- Plum Island Animal Disease Center (PIADC)** The PIADC, located on a 180 acre site off the northeastern tip of Long Island, New York, is part of the Department of Homeland Security’s efforts to protect the United States’s food supply. PIADC efforts work to protect U.S. consumers and safeguard the integrity of U.S. animal product exports against catastrophic economic losses caused by biologic agents accidentally or deliberately introduced by terrorists.
- PMOI** People’s Mujahidin of Iran.
- PNG** Pseudorandom number generator.
- P-note** A counterfeit banknote produced with a computer printer.

- POG** Hizballah (Party of God).
- Polarization** Plane of vibration of an electrical signal (the orientation of a signal's electrical field).
- Politburo** The central policy-making and governing body of the USSR Communist Party.
- Polybius square** A grid in which letters of the alphabet are arranged in a square such that each letter has a unique position identifiable by the numbers of its row and column.
- PORTPASS** The Port Passenger Accelerated Service System (PORTPASS) is a generic term for programs developed to expedite passage through U.S. national entry systems. PORTPASS components include the INSPASS (Immigration and Naturalization Service Passenger Accelerated Service System), SENTRI (Secure Electronic Network for Travelers' Rapid Inspection), OARS (Outlying Area Reporting Station), and RVIS (Remote Video Inspection System) systems.
- POTUS** President of the United States.
- Power** For many electronic devices this term denotes power required or consumed by operation. Often, however, the term "power" denotes a specialized contextual or application-related meaning (e.g., with regard to a signal transponder it commonly refers to signal amplification power).
- PRC** People's Republic of China.
- Presidential directive** A classified set of guidelines or rules issued by the President of the United States, usually in reference to some sensitive issue such as security or intelligence.
- Primary RADAR** RADAR systems that receive reflections of their own transmitted signals as returned signals from the target.
- Principal agent** An agent who performs the role of surrogate handler, working over other agents and reporting to an intelligence officer.
- Profiling** The process of developing descriptions of the traits and characteristics of unknown offenders in specific criminal cases.
- Propaganda** A form of communication that attempts to influence the behavior of people by affecting their perceptions, attitudes and opinions.
- Propagation** Traveling or penetration of waves through a medium.
- Prophylaxis** Pre-exposure treatments (e.g., immunization) that prevents or reduces severity of disease or symptoms upon exposure to the causative agent.
- Protein** Macromolecules made up of long sequences of amino acids.
- Pseudoscience** (false science) Arguments or ideas, often laced with scientific terminology or bizarre calculations, based on theories developed outside of the scientific method and thus not subject to scientific validation.
- PSI** Personnel security investigation.
- Psychological warfare** The use of tools and techniques designed to influence the views of allies, enemies, and neutrals. Propaganda is a major component of psychological warfare, which includes other facets such as displays of force, and contrasting positive and negative treatment of detainees—known colloquially as "good cop/bad cop."
- Psychotropic drugs** A loosely defined grouping of agents that have effects on psychological function and include antidepressants, hallucinogens, and tranquilizers. They are all compounds that affect the functioning of the mind through pharmacological action on the central nervous system.
- Public Health Service, United States** A federal government agency that promotes the health of the people of the United States and the world. It is a principle component of the Department of Health and Human Services (HHS) and is composed of eight agencies. Among other duties, the Public Health Service is charged with, through its agencies, preparing for and leading the nation's medical response to a threat or disaster, whether naturally occurring or an act of terrorism.
- Public key cipher** Cipher system which allows the exchange of enciphered messages without prior distribution of secret keys to all users. Each user calculates their own secret key and uses it in combination with a public key to send and receive messages.
- Purple Machine** An Allied codename for one of several Japanese cipher machines used during World War II.
- Puzzle Palace** Nickname for the NSA (United States National Security Agency).
- QI/ST** Quantum Information Science and Technology.
- Radar** Radar—an acronym for *RA*dio *D*etection *A*nd *R*anging—is the use of electromagnetic waves at sub-optical frequencies (i.e., less than about  $10^{12}$  Hz) to sense objects at a distance.
- RADAR, synthetic ap** Synthetic aperture RADAR (SAR) is used for high-resolution mapping of the ground from moving aircraft or spacecraft.
- RADINT** Radar intelligence from nonimaging radar. Unlike ELINT, RADINT does not involve the interception of radar signals; instead, intelligence regarding flight path and other specifics is derived from the deflection of enemy radar signals. RADINT is a subcategory of MASINT, or measurement and signatures intelligence.
- Radio frequency (RF) weapons** RF weapons, also known as directed-energy weapons, use electromagnetic energy on specific frequencies to disable electronic systems. The principle is similar to that of high-power microwave (HPM) weapons, only HPM systems tend to be much more sophisticated, and are thus, more likely to be in the control of superpowers or near-superpowers. RF weapons, by contrast, are simple and low-voltage enough that they could be deployed by smaller, less technologically enhanced forces.
- Radiological** Having to do with nuclear radiation.
- Radiomimetic** An agent or exposure protocol that simulates radioactive exposure.
- RAID** Real-time Analytical Intelligence Database.
- RASCAL** Responsive Access, Small Cargo, Affordable Launch.
- RCS** Radar Cross Section.
- RDD** Radiological dispersal device, often called a "dirty bomb."

- Recombinant DNA** DNA that is cut using specific enzymes so that a gene or DNA sequence can be inserted.
- Reconnaissance** A term for efforts to gain information about an enemy, usually conducted before, or in service to, a larger operation.
- Red code** A Japanese naval code created during World War I and used until the outbreak of World War II. The Red code used the additive encryption method.
- Red Scare** Period of anticommunist hysteria in United States from 1918–1920, culminating in the Palmer Raids; also invoked to describe the resumption of anticommunist activities in the late 1940s and early 1950s.
- Redoubled agent** A double agent whose activities have been discovered by the agency against which he or she is spying, and who is then used—either wittingly or unwittingly, willingly or unwillingly—in that agency’s service against the other.
- Refractive index** (characteristic of a medium) Degree to which a wave is refracted, or bent.
- Remote sensing** The acquisition of information about an object or phenomenon by a device located a considerable distance from the object or phenomenon.
- Resolution** The ability of a sensor to detect objects of a specified size. The resolution of a satellite sensor or the images that it produces refers to the smallest object that can be detected.
- Retina and iris scans** Scans that detect and map the neural part of the eye responsible for vision. The pattern of blood vessels serving the retina is as unique as fingerprints.
- RF** Radio frequency.
- RF detection** RF, or radio frequency systems are directed-energy weapons that use electromagnetic energy on specific frequencies to disable electronic systems.
- RF weapons** Radio frequency weapons, also known as directed-energy weapons, which use electromagnetic energy on specific frequencies to disable electronic systems.
- RHD** Red Hand Defenders.
- Richter scale** Scale used to measure the intensity of seismic events, or earthquakes.
- Ricin** A highly toxic protein that is derived from the bean of the castor plant (*Ricinus communis*). The toxin causes cell death by inactivating ribosomes, which are responsible for protein synthesis. Ricin can be produced in a liquid, crystal or powdered forms and it can be inhaled, ingested, or injected. It causes fever, cough, weakness, abdominal pain, vomiting, diarrhea, dehydration, and death. There is no cure for ricin poisoning.
- Ring** A group or network.
- RIRA** Real IRA.
- RJO** Revolutionary Justice Organization.
- RN group (Greece)** Revolutionary Nuclei.
- RNA** Ribonucleic acid.
- Rogue state** A nation that harbors terrorists and poses a serious security threat to its neighbors.
- RPA** Revolutionary Proletarian Army.
- RTH** Radioactive thermoelectric generators.
- RUF** Revolutionary United Front.
- RVIS** Remote Video Inspection System.
- S&T** Directorate of Science and Technology (S & T), Department of Homeland Security.
- Sabotage** A deliberate act of destruction or work stoppage intended to undermine the activities of a larger entity, whether it is a business, government, or some other organization. The practice of sabotage, which has roots in the labor movements of the late nineteenth and early twentieth centuries, gained military and political application during the world wars and thereafter. It has also been a part of covert operations, often undertaken by agents provocateur.
- Safe house** Any precleared or secret building where agents can meet or operate without detection.
- SAIP** Semi-Automatic IMINT Processing Systems.
- SANDKEY** NSA Analysis and Reporting software.
- Sanitize** To delete sensitive or classified information prior to release.
- SAR** Search and rescue.
- SAR** Synthetic Aperture Radar.
- Sarin gas** Sarin gas (O-Isopropyl methylphosphonofluoride), also called GB, is a dangerous and toxic chemical. It belongs to a class of chemical weapons known as nerve agents, all of which are organophosphates. The G nerve agents, including tabun, sarin and soman, are all extremely toxic, but not very persistent in the environment. Pure sarin is a colorless and odorless gas, and since it is extremely volatile, can spread quickly through the air.
- SARS** Severe Acute Respiratory Syndrome.
- S-band** 2.700–3.500 GHz.
- SBCOM** United States Army Soldier and Biological Chemical Command.
- SB-WASS** Space Based Wide Area Surveillance.
- Scalable** The degree to which an algorithm is capable of implementing additional computational resources in such a way as to solve increasingly more complex problems. To be truly scalable, the work required to solve an algorithm should grow at a rate smaller than the rate at which the amount of input grows.
- Scientific intelligence** Intelligence on the development of new weapons or techniques by an enemy. Closely related to TECHINT, or technical intelligence.
- SDI** Strategic Defense Initiative.
- SDNS** Secure Data Network System [NSA].
- SDS** Surveillance Direction System.
- SEAL teams** U.S. Navy Sea-Air-Land (SEAL) Teams (special forces).
- SEASAT** Ocean surveillance satellite.
- Secret** The second highest U.S. general security classification. A term referring both to information whose disclosure to unauthorized personnel could reasonably be expected to cause serious damage to national security, and to the security clearance necessary to access such information.

- Secret agent** An agent who works in a clandestine capacity, such that the relationship with the intelligence agency is not obvious to those around him or her. Also known as an undercover agent.
- Secret writing** Any means of written communication whereby a spy conceals the actual written text, whether it be enciphered/encoded or not. Codes and ciphers are sometimes mistakenly placed under the heading of “secret writing,” but this is accurate only if that expression is taken in its most general sense, as writings that are concealed in any way. Whereas codes and ciphers conceal the meaning of a message, secret writing conceals the actual message.
- Security clearance** A limited license or initial general permission to access classified information—that is, any data or material belonging to the federal government that relates to sensitive topics such as military plans or vulnerabilities of security systems.
- Secret Spoke** An Echelon security compartment equivalent to the general security level designation “Confidential.”
- Seismogram** The visual record of earthquake vibrations or waves produced by a seismograph, which is an instrument capable of sensing and recording the waves.
- Seismograph** An instrument that measures and records elastic ground vibrations called seismic waves that are generated by earthquakes and man-made explosions. Seismology has been an important tool for the remote detection of large explosions, especially underground nuclear tests, for many years and is expected to play an important role in Comprehensive Test Ban Treaty verification.
- Sendero Luminoso** Shining Path, or SL.
- Sensitive Compartment Information (SCI)** Data concerning sophisticated technical systems for collecting intelligence, as well as information collected by those systems, access to which requires a special security clearance.
- SENTRI** Secure Electronic Network for Travelers’ Rapid Inspection.
- SF 86** Standard Form 86, a “Questionnaire for National Security Positions” that federal employees, military personnel, and contractors must complete in order to gain a security clearance.
- SFAI** Swept Frequency Acoustic Interferometer.
- Shin Bet** The Israeli intelligence agency.
- Shin Beth** The Israeli counterintelligence service.
- Shining Path** Sendero Luminoso (Shining Path, or SL).
- Short wave** Radio frequencies ranging from the upper limit of the AM band to the lower limit of the VHF (television) band (1605 kHz to 54 MHz).
- Short-wave transmissions** Radio transmissions in the range somewhere between 2 and 30 MHz (megahertz, or million cycles per second). Because these signals are capable or propagating over a greater distance than either AM or FM radio, shortwave is the preferred medium for radio broadcasting to remote locations.
- SIDR** Secure Intelligence Data Repository.
- SIGINT** Signals intelligence, or intelligence derived from the interception of signals, including communications signals, electronic emissions, and telemetry. The two major subsets of SIGINT are COMINT or communications intelligence, and ELINT or electronics intelligence. SIGINT, is one of the four major forms of intelligence, along with human, imagery, and measurement and signatures intelligence (HUMINT, IMINT, and MASINT respectively).
- Signature** In the MASINT context, *signature* refers to characteristic markings, such as the auditory signature of a submarine detected on sonar.
- Silencer** A device contrived to suppress sound by means of an attachment to a firearm.
- SIPRNET** Secret Internet Protocol Router Network.
- SIS** Signal Intelligence Service, the U.S. Army group responsible for deciphering Japanese diplomatic codes during World War II.
- Skunk Works** The nickname for the headquarters of advanced development programs for Lockheed Martin Aeronautics Company at Palmdale, California, some 80 miles (128 km) north of Los Angeles in the Antelope Valley. Established in 1943 by what was then known as the Lockheed Aircraft Corporation, the Skunk Works has been the birthplace of numerous extraordinary aircraft, including the U-2 and SR-71 reconnaissance planes, and the F-117A stealth fighter.
- SL** Sendero Luminoso (Shining Path, or SL).
- SLBM** Submarine-launched ballistic missile.
- Sleeper agent** An agent placed in an undercover situation and told to await further instructions before beginning to actively engage in espionage activities. A sleeper may remain inactive for months or years, or even the rest of his or her life.
- Smallpox** An infection caused by the variola virus, a member of the poxvirus family. The disease is highly infectious. Passage from person to person via contaminated aerosolized droplets (from sneezing, for example) occurs easily, and so the spread of smallpox through a population can occur quickly.
- Smart card** A card with biometric and other data contained in an embedded microchip or other form of integrated circuitry.
- SMERSH** A KGB assassination team (*SMERrt SHpionam* or “Death to Spies”).
- SMPAS** Space Mission Payload Assessment System.
- SOE** Special Operations Executive.
- SOF-IV** Special Operations Forces—Intelligence Vehicle.
- Solid phase microextraction techniques (SPME)** A chemical technique designed to detect chemical compounds. In its forensic application, it is used to find chemical warfare agents, high explosives, or illegal drugs.
- Soman** Soman (or “GD”) is a synthetic (human-made) compound that affects the functioning of nerves. As such, soman is one of a group of chemicals (e.g., tabun) that are known as nerve agents.
- SONAR** Sound Navigation and Ranging (SONAR) is a remote sensing system with important military, scientific and commercial applications. Active SONAR transmits acoustic (i.e., sound) waves. Passive SONAR is a listening mode to detect



- noise generated from targets. SONAR allows the determination of important properties and attributes of the target (i.e., shape, size, speed, distance, etc.).
- SOSUS** Sound Surveillance System.
- Special agent** A term for operatives of the Federal Bureau of Investigation (FBI) during the leadership of J. Edgar Hoover and thereafter. By this designation, Hoover meant to distinguish FBI agents from ordinary police officers.
- Special Operations Executive (SOE)** The British Special Operations Executive, created in 1940, was given the mission to “set Europe ablaze.” The SOE supplied and organized resistance cells in Nazi-occupied Europe, carrying out missions of intelligence gathering, sabotage, and other covert activities.
- Special relationship** During World War II, the intelligence services of the United States and the United Kingdom worked together in their efforts against the Axis powers, particularly in Europe, and formalized the collaboration with agreements in 1943 and 1946.
- Spectra** Low-frequency collection system used by the Navy.
- Spectroscopy** The measurement of the absorption, scattering or emission of electromagnetic radiation by atoms or molecules.
- Spook** An American term for an intelligence officer or agent.
- Spore** A hard casing that contains the genetic material of those bacteria and other microorganisms that are able to form the structure. This physically and chemically resilient package protects the genetic material during periods when the environmental conditions are so harsh that the growing form of the microbe would be killed.
- SPOT** A French satellite, *System Probatoire d’Observation de la Terre*.
- SPR** Strategic Petroleum Reserve.
- Spread spectrum** A radio signal spread out across a range of frequencies to evade detection and decoding.
- SR-71** A SR-71 spy plane is a black-colored, high-altitude airborne reconnaissance platform.
- SSA** Signal Security Agency.
- SSCI** United States Senate Select Committee on Intelligence.
- SST** Space Surveillance Telescope.
- START** Strategic Arms Reduction Treaty.
- Stasi** The *Ministerium für Staatssicherheit*, Ministry of State Security, was the primary intelligence and security agency of the German Democratic Republic (GDR), or East Germany, during the cold war.
- Static address** A permanent Internet protocol (IP) address that uniquely identifies a computer connected to the Internet.
- StB** (Statni Bezpecnost) The “secret police” of Czechoslovakia before 1990.
- Stealth technology** Stealth technology, also termed “low-observable” technology, is a set of techniques that render military vehicles, mostly aircraft, hard to observe. Because RADAR—an acronym for *RA*dio *D*etection *A*nd *R*anging—is the primary detection technology for aircraft, most stealth technologies are directed at suppressing RADAR returns from and infrared observation of aircraft.
- Steganography** (from the Greek for “covered writing”). The secret transmission of a message. It is distinct from encryption, because the goal of encryption is to make a message difficult to read while the goal of steganography is to make a message altogether invisible.
- STICS** Scalable Transportable Intelligence Communications System [NSA].
- Stinger** A nickname for two very different weapons. The first, a 22-caliber pistol that could be hidden in a toothpaste tube, was used by the CIA after World War II. The second, developed by General Dynamics in the 1970s, was a surface-to-air missile used most notably by Afghan *mujahideen* against the Soviets in the 1980s.
- Strategic Arms Limitation Treaty (SALT)** A series of treaties begun in 1972 that limited the number of long-range offensive missiles held by the United States and the Soviet Union.
- Strategic geologic intelligence** The geologic or geotechnical information necessary to evaluate the vulnerability of an underground facility to attack.
- Strategic metal** A metal that is essential for industry and national security, but for which a nation has little or no domestic supply. The ores of strategic metals are often referred to as strategic minerals.
- Strategic Petroleum Reserve (SPR)** The SPR, located in the United States and operated by the Department of Energy (DOE), is the largest emergency supply system of oil in the world.
- Stream cipher** Stream ciphers operate upon a series of binary digits (“bits,” usually symbolized as 1s and 0s), enciphering them one by one rather than in blocks of fixed length.
- Stringer** A freelance agent who works periodically or occasionally for an intelligence agency.
- Strong encryption** A method of encryption in which a cipher is unbreakable, or virtually unbreakable, without knowledge of the key.
- Suitcase bomb** A small, portable nuclear weapon, usually weighing less than 100 pounds, that can be transported and hidden in a suitcase or other small container.
- Superfund Program** Established by the United States Congress in 1980 to locate, investigate, and clean up the worst toxic waste sites nationwide.
- Supreme Truth** Aum Supreme Truth (Aum) Aum Shinrikyo, Aleph.
- Surveillance** Intelligence-gathering observations made regularly or continuously in order to monitor an area of interest for changes.
- SVR** Russian foreign intelligence.
- SZ42 cipher machine** A cipher machine used by Germany in WWII. The German military did not replace Enigma with the SZ42 for general use because the SZ42’s complexity made it too heavy for the field.
- Tabun** Tabun (or “GA”, O-ethyl N,N-dimethylphosphorodiamidocyanide) is one of a group of synthetic chemicals that

- were developed in Germany during the 1930s and 1940s (tabun was developed in 1936). The original intent of these compounds, including tabun, was to control insects. However, tabun and the other human-made nerve agents proved to be much more potent than the organophosphates, and so quickly became attractive as chemical weapons.
- Tapping** The clandestine physical interception of electronic messages, especially telephone conversations and messages.
- Targeting** The prioritization of certain target areas or facilities for possible military or intelligence action.
- TECHINT** Technical intelligence, or intelligence relating to the technical abilities of an enemy. TECHINT does not fall under just one of the four major branches of intelligence; rather, it includes elements of imagery, measurement and signatures, and signals intelligence (IMINT, MASINT, and SIGINT respectively).
- TECS** Treasury Enforcement Communication System.
- Telemetry** The process of making measurements from a remote location and transmitting those measurements to receiving equipment.
- TELINT** Telemetry intelligence, an example of which is the use of signals to relay information on the performance of a guided missile system. TELINT is a subset of FISINT (foreign instrumentation signals intelligence), which is in turn a subcategory of ELINT, or electronic intelligence.
- TERPES** Tactical Electronic Reconnaissance Processing and Evaluation System.
- Terrorism** The systematic belief in the political, religious, or ideological efficacy of producing fear by attacking—or threatening to attack—unsuspecting or defenseless populations, usually civilians, and usually by surprise.
- THAAD** Theater High Altitude Area Defense.
- Thin layer chromatography** Thin layer chromatography, which is typically abbreviated as TLC, is a type of liquid chromatography that can separate chemical compounds of differing structure based on the rate at which they move through a support under defined conditions.
- TIA** Total Information Awareness.
- TIARA** Tactical Intelligence and Related Areas, an annual budget request for specific tactical intelligence requirements of the military services, presented by the Secretary of Defense to the President of the United States.
- TIFG** Tunisian Islamic Fighting Group.
- TMD-GBR** Theater Missile Defense-Ground Based Radar.
- TNT** The explosive, trinitrotoluene.
- Top Secret** The highest general U.S. security classification. Other restrictions include “need to know access.” Top secret refers to information whose disclosure to unauthorized personnel could reasonably be expected to cause exceptionally grave damage to national security, and to the security clearance necessary to access such information.
- Top Secret Umbra** An Echelon security compartment equivalent to the general security level designation “Top Secret.”
- Topographic map** A map reflecting the shape, or topography, of Earth’s surface. Topography can be depicted using contour lines of equal elevation or by using shading techniques to simulate a three dimensional surface.
- Toxicity** The degree to which a chemical, in sufficient exposure, can poison humans or other organisms.
- Toxicology** The science of toxicology is concerned with the adverse effects of chemicals on biological systems and includes the study of poisons, their detection, action and counteractions. Toxicologists today generally use the techniques of analytical chemistry to detect and identify foreign chemicals in the body, with a particular emphasis on toxic or hazardous substances.
- Toxin weapons** A poison produced by a living organism, or its derivative.
- Tradecraft** Techniques of the espionage trade, or the methods by which an agency involved in espionage conducts its business.
- Transducer** An instrument that that converts one type of energy into another.
- Transmutation** The conversion of one nuclide into another, as by neutron bombardment in a nuclear reactor.
- Transponder** Integrated operation of receivers, frequency converters, and transmitter devices.
- Triangulation** A means of navigation and direction finding based on the trigonometric principle that, for any triangle, when one side and two angles are known, the other two sides and triangles can be calculated.
- Trojan horse** A security-breaking program, disguised as a benign product, that is designed for the purpose of clandestinely introducing itself into a remote user’s computer, and then wreaking havoc in one way or another.
- Truth drugs** Anesthetics employed in interrogation that are intended to act as truth serums.
- Truth serum** A term given to any of a number of different sedative or hypnotic drugs that are used to induce a person to tell the truth. Truth serums cause a person to become uninhibited and talkative, but they do not guarantee the veracity of the subject.
- TSA** Transportation Security Administration (previously part of the Department of Transportation). On March 1, 2003, agents were transferred to the Department of Homeland Security (DHS), directorate of Border and Transportation Security (BTS).
- Tularemia** A plague-like disease caused by the bacterium *Francisella tularensis*.
- Typex** The name for the principal encryption device, or cipher machine, used by the military, intelligence, and diplomatic services of the British Empire during World War II.
- UDA/UVF** Ulster Defense Association/Ulster Freedom Fighters (UDA/UVF).
- UFO (Unidentified Flying Object)** A flying object of unknown origin, popularly but unscientifically assumed to be associated with extraterrestrial beings or paranormal phenomena. Most often, UFOs are explained by weather phenomena or military aircraft.
- UHF-band** 0.430–1.300 GHz.
- Ultra** Operation Ultra was the codename for the British cryptologists efforts at Bletchley Park to intercept and break

- German coded messages. While Ultra initially was the cryptonym for the project to break the German Enigma machine, the code name came to represent all British efforts to break high-level German radio codes during World War II.
- Umbra Gamma** An Echelon security compartment equivalent to the general security level designation "Secret."
- UN** United Nations.
- Undercover agent** An agent who works in a clandestine capacity, such that the relationship with the intelligence agency is not obvious to those around him or her. Also known as a secret agent.
- Unified command principle** The idea, which emerged in U.S. military circles during the late 1980s and began to prevail in the early 1990s, that unified or area commanders in chief should direct all U.S. military operations in a given geographic area.
- UNMOVIC** United Nations Monitoring, Verification and Inspection Commission.
- Uplink** An Earth to satellite connection or electronic signal path.
- Uranium depletion weapons** Depleted uranium (DU) munitions are armor-piercing or general-purpose ammunition rounds that are composed, in part, of depleted uranium. Depleted uranium is uranium that has had most of its <sup>234</sup>U and <sup>235</sup>U removed for use in nuclear power or nuclear weapons, leaving metal that is almost entirely <sup>238</sup>U.
- Urticant** A compound that produces excessive skin irritation and itching.
- USA** United States Army.
- USAF** United States Air Force.
- USAMRICD** Army Medical Research Institute of Chemical Defense, United States.
- USAMRIID** United States Army Medical Research Institute of Infectious Diseases. The facility is operated by the Department of Defense and serves as the country's principle laboratory for research into the medical aspects of biological warfare.
- USCG** United States Coast Guard.
- USCSB** United States Chemical Safety and Hazard Investigations Board.
- USIGS** United States Imagery and Geospatial Information Systems Architecture.
- USIS** United States Imagery System Architecture.
- USMC** United States Marine Corps.
- USN** United States Navy.
- USOGE** United States Office of Government Ethics.
- USPS** United States Postal Service.
- USSR** Union of Soviet Socialist Republics.
- USSS** United States SIGINT System.
- USSTRATCOM** United States Strategic Command.
- UUV** Unmanned undersea vehicles.
- UVF** Ulster Freedom Fighters.
- V-agents** A group of alkyl esters of S-dialkylamino ethylmethylphosphonothioic acids that are nerve agents.
- Venona** The Venona Project was the United States Army's Signal Intelligence Service, and later the National Security Agency's, operation to intercept and decrypt high-level Soviet diplomatic communications.
- VERS** The Vaccine Event Reporting System is a U.S. vaccine safety surveillance program that is under the direction of the Food and Drug Administration and the Centers for Disease Control and Prevention.
- Viruses** Nonliving repositories of nucleic acid that require the presence of a living prokaryotic or eukaryotic cell for the replication of the nucleic acid. There are a number of different viruses that challenge the human immune system and that may produce disease in humans. In common, a virus is a small, infectious agent that consists of a core of genetic material (either deoxyribonucleic acid [DNA] or ribonucleic acid [RNA]) surrounded by a shell of protein.
- VOA** Voice of America.
- Vozrozhdeniye Island** A Russian island located in the Aral Sea approximately 1,300 miles to the east of Moscow that was used as a bioweapons test facility for the former Soviet Union.
- VR** Virtual reality.
- Vulnerability assessment** A test of a system to locate, diagnose, and correct areas of weakness that might make it susceptible in times of crisis, attack, or destabilization.
- VX agent** VX nerve agent (O-ethyl S-[2-diisopropylaminoethyl] methylphosphonothioate) is an organophosphate. Although it is often called a nerve gas, VX is usually a clear, odorless, tasteless liquid. A tiny amount of VX, about 10 mg, absorbed through the skin, eyes, or ingested is fatal, and death usually occurs within an hour of exposure.
- WAN** Wide Area Network.
- Watchers** Specialized intelligence personnel who maintain surveillance on targeted individuals.
- Watermarking** The impression of a subtle pattern on paper using water. A watermark is only visible when the paper is held up to a light.
- Watershed** The area contributing water to a river, stream, lake, or ocean. Watersheds can be defined on several scales ranging from hundreds of square meters to millions of square kilometers.
- Weapons of mass destruction** Weapons that cause a high loss of life within a short time span. Nuclear, chemical, and biological weapons are classified as weapons of mass destruction.
- Weapons-grade material** Weapon-grade (or "bomb-grade") uranium or plutonium is any alloy or oxide compound that contains enough of certain isotopes of these elements to serve as the active ingredient in a nuclear weapon.
- Whistle-blower** A person inside an organization such as a corporation or government agency who comes forward with evidence of wrongdoing by the organization.
- WHO** World Health Organization.

**Windtalkers** The code name given to the Navajo Indian code talkers employed by United States military intelligence during World War II. Agents developed several encryption methods and code systems during the war, but a code based on the ancient Navajo language was one of the most successful codes ever used. It remained unbroken throughout the course of the war.

**Wiretapping** The act or instance of breaking into a telephone line to monitor a conversation or conversations. Wiretapping

is usually illegal, though it may be applied by law-enforcement organizations with a search warrant.

**WMD** Weapons of mass destruction.

**World Islamic Front for Jihad** A group absorbed by Al-Qaeda (also known as Al-Qaida).

**Yperite** Mustard agent or gas.

**Zoonoses** Diseases transmitted from animals.

*This page intentionally left blank*

## Chronology

- c. 6000 B.C. The rise of the great ancient civilizations, beginning 6,000 years ago in Mesopotamia, begat institutions and persons devoted to the security and preservation of their ruling regimes and founded the need for espionage, intelligence, and security operations.
- c. 3500 B.C. Underground passages first used as hiding places and escape routes during times of war.
- c. 1980 B.C. Egyptian pharaoh Amenemhet I is targeted as one of the first recorded victims of political assassination.
- c. 1500 B.C. Between 1500 B.C. and 1200 B.C., Greece's many wars with its regional rivals lead to the development of new military and intelligence strategies. The early Greeks relied on deception as a primary means of achieving surprise attacks on their enemies.
- c. 1000 B.C. From 1,000 B.C. onwards, Egyptian espionage operations focused on foreign intelligence about the political and military strength of rivals Greece and Rome. Egyptian spies were the first to develop the extensive use of poisons, including toxins derived from plants and snakes, to carry out assassinations or acts of sabotage.
- c. 500 B.C. Chinese military logician Sun-tzu stresses the importance of intelligence gathering and deception in his treatise *The Art of War*. In this work, added to by later philosophers, Sun-tzu detailed methods of espionage that included the use of defectors, double agents, and organized spy rings.
- c. 480 B.C. Demaratus of Sparta uses an early form of secret writing, concealing a message on a wooden tablet covered with wax to warn his countrymen of invasion by the Persian empire.
- c. 400 B.C. The Spartans use a cryptographic system called a *scytale* on papyrus wrapped around wooden scrolls.
- c. 400 B.C. Tunneling first used in warfare.
- c. 300 B.C. *Arthashastra*, an ancient Indian manual on politics, discusses mining, metallurgy, medicine, pyrotechnics, poisons, and fermented liquors.
- c. 300 B.C. During the Etruscan wars, Roman consul Fabius Maximus sends his brother to spy on Umbrians. Romans develop use of intelligence to gain treaties and scout military forces.
- 44 B.C. Assassination of Julius Caesar; records have established that the Roman intelligence community knew of the plot and even provided information to Caesar or his assistants providing the names of several conspirators. In a pattern to be repeated throughout the ages, the information from the intelligence community was ignored.
- c. 100 A.D. Roman records dating to the first century mention the presence of a secret police force, the *frumentarii*.
- c. 900 A.D. Lack of records conceals facts of espionage during the Middle Ages, but the birth of large nation-states, such as France and England, in the ninth and tenth centuries facilitated the need for intelligence in a diplomatic setting.
- 1095 Pope Urban II calls for the first Crusade, a military campaign to recapture Jerusalem and the Holy Lands from Muslim and Byzantine rule. Over the next four centuries, the Catholic Church masses several large armies, and employs spies to report on defenses surrounding Constantinople and Jerusalem. Special intelligence agents also infiltrate prisons to free captured crusaders, and sabotage rival palaces, mosques, and military defenses.
- c. 1200 Thirteenth-century Church councils establish laws regarding the prosecution of heretics and anti-clerical political leaders. The ensuing movement became known as the Inquisition. Espionage was an essential component of the Inquisition. The Church relied on vast networks of informants to find and denounce suspected heretics and political dissidents.
- 1245 A Franciscan monk, Carpini, is used by Pope Innocent IV to gather intelligence about Mongols.
- 1520 Niccolo Machiavelli, a Florentine political philosopher, publishes a series of book detailing the qualities and actions of effective rulers. In his works, *The Prince*, and *The Art of War*, Machiavelli advocates that rulers routinely employ espionage tradecraft,

- engaging in deception and spying to insure protection of their power and interests. His advice, much of which was culled from rediscovered works of Aristotle and Cicero, was intended for the ruling Medici princes of Florence. However, the works gained popularity several centuries after their 1520 publication.
- c.1550 Henry VIII and his daughter Elizabeth I nurture a spy network to locate and infiltrate Catholic loyalist cells that threaten the English monarchy. The Elizabethan intelligence community employs linguists, scholars, authors, engineers, and scientists, relying on professional experts to seek and analyze intelligence information.
- 1574 Francis Walsingham, joint secretary of state under Queen Elizabeth I of Britain, mounts an elaborate and effective spy network that uncovers a plot against Elizabeth by the imprisoned Mary, Queen of Scots, who was then executed. Later, in 1587, the spy network provides Elizabeth with information warning of the impending attack of the Spanish Armada.
- 1593 Christopher Marlowe, English dramatist/playwright/poet, is murdered in a Deptford tavern after being accused of being a spy.
- c.1600 Chemists invent invisible inks, and the rebirth of complex mathematics revives long-dormant encryption and code methods. Later, in the Scientific Revolution and the Enlightenment, the development of telescopes, magnifying glasses, the camera obscura, and clocks facilitates remote surveillance and the effective use of "dead drops" to pass information between agents.
- 1670 Secret treaty between Charles II and Louis XIV.
- c.1700 The Age of Empires: espionage further develops in the numerous conflicts and wars that occur in Europe and between rival colonial powers in Europe and abroad. Industrialization, economic and territorial expansion, the diversification of political philosophies and regimes, and immigration all transform the world's intelligence communities.
- 1703 Although concepts of disease are primitive, in an act of biological warfare, Sir Jeffrey Amherst, commander-in-chief of British forces in North America, suggests grinding the scabs of smallpox pustules into blankets intended for Native American tribes known to trade with the French.
- 1776 Benjamin Thompson (Count Rumford), an English physicist whose work contributed to the formulation of the second law of thermodynamics, acts as Tory spy during the American Revolution.
- 1776 Nathan Hale hanged by the British as a spy during the American Revolution. His last words are reputed to have been, "I only regret that I have but one life to give for my country."
- 1780 General Benedict Arnold betrays the colonial revolution when he promises secretly to surrender the fort at West Point to the British army. Arnold flees to England; his co-conspirator, British spy Major John Andre, is hanged.
- 1789 Congress passes the Judiciary Act, which establishes the federal justice system and creates the Office of the Attorney General, as well as the U.S. Marshal Service.
- 1789 U.S. Customs Service begins operation on July 31.
- 1789 Congress establishes the Department of State on September 15.
- 1789 French spy Richeborg (a dwarf) is disguised as a baby in diapers, and carried in girl's arms, so he can eavesdrop on conversations and carry secret letters through Paris during the French Revolution.
- 1789 During the French Revolution, Robespierre's informant networks denounce traitors to the new republic and track down refugee aristocrats and clergy for trial and execution. The wide application of treason charges marks one of the greatest abuses of intelligence powers in the modern era.
- 1790 France introduces the metric system.
- 1794 First army air corps established when revolutionary France creates a military balloon contingent.
- 1795 Martin Heinrich Klaproth, German chemist, isolates a new metal and names it titanium, after the Titans of Greek mythology. He gives full credit to English mineralogist William Gregor, who first discovered it in 1791.
- 1798 Government legislation is passed to establish hospitals in the United States devoted to the care of ill mariners. This initiative leads to the establishment of a hygienic laboratory, which eventually grows to become the National Institutes of Health.
- 1798 Geologists accompany Napoleon's expeditionary force to Egypt.
- 1798 U.S. Congress establishes the Department of the Navy, which also includes the Marine Corps.
- 1799 Chinese emperor Kia King's ban on opium fails to stop the lucrative British opium trade.
- 1800 Records indicate use of chloral hydrate in the "Mickey Finn," an anesthetic cocktail used to abduct or lure sailors to serve on ships bound for sea.
- 1800 Alessandro Giuseppe Antonio Anastasio Volta, Italian physicist, announces his invention of the voltaic pile, which is the first battery. His work duplicating Galvani's 1791 "animal electricity" experiment leads him to discover that it is the contact of dissimilar metals that causes the electricity. He arranges suitable pairs of metallic plates in a certain order, separates them by pieces of leather soaked in brine, and creates a pile, or battery, that produces a continuous and controllable electric current.
- c.1800 Colonial rulers and powers employ secret police and agents of espionage throughout their territorial holdings, hoping to quell anti-colonial rebellions and separatist movements.
- 1802 John Dalton introduces modern atomic theory into the science of chemistry.
- 1804 Joseph Fouché, a French revolutionary and minister of police, sets up the first modern police state, and uses his spy network to uncover and foil a plot by George Cadoudal against Napoleon Bonaparte.

- 1805 Joseph-Louis Gay-Lussac, French chemist, establishes that precisely two volumes of hydrogen combine with one volume of oxygen to form water.
- 1812 Second U.S. war with Great Britain, commonly called the War of 1812.
- 1817 German pharmacist Frederick Serturmer announces the extraction of morphine from opium.
- 1818 Augustin-Jean Fresnel, French physicist, publishes his *Mémoire sur la diffraction de la lumière* in which he demonstrates the ability of a transverse wave theory of light to account for such phenomena as reflection, refraction, polarization, interference, and diffraction patterns.
- 1820 André Marie Ampère, French mathematician and physicist, extends Ørsted's work and formulates one of the basic laws of electromagnetism.
- 1823 Monroe Doctrine declares Western Hemisphere a U.S. "sphere of influence."
- 1827 Georg Simon Ohm, German physicist, experiments with electricity using wires of different length and diameter and discovers that a long, thick wire passes less current than a short, thin wire. He states what becomes Ohm's law.
- 1828 Friedrich Wöhler synthesizes urea. This is generally regarded as the first organic chemical produced in the laboratory, and an important step in disproving the idea that only living organisms can produce organic compounds. Work by Wöhler and others establish the foundations of organic chemistry and biochemistry.
- 1828 Luigi Rolando, Italian anatomist, achieves the first synthetic electrical stimulation of the brain.
- 1831 Michael Faraday, English physicist and chemist, discovers electromagnetic induction. After laboring for ten years to achieve the opposite of what Ørsted had done—to convert magnetism into electricity—he finally produces for the first time an induction current using a magnet. This is the first electric generator. With such a device, mechanical energy can be converted into electrical energy.
- 1837 Invention of the Daguerreotype, the first practical form of photography. When widely incorporated into intelligence practices in the 1860s, the photograph permitted agents of espionage to portray targets, documents, and other interests.
- 1839 First Opium War begins between Britain and China. The conflict lasts until 1842. Imperial Chinese commissioner Lin Tse-hsü seizes or destroys vast amounts of opium, including stocks owned by British traders. The result was a Chinese payment of an indemnity of more than 21 million silver dollars and Hong Kong being ceded to Britain under the Treaty of Nanking.
- 1839 Theodore Schwann extends the theory of cells to include animals and helps establish the basic unity of the two great kingdoms of life. He publishes *Microscopical Researches into the Accordance in the Structure and Growth of Animals and Plants*, in which he asserts that all living things are made up of cells, and that each cell contains certain essential components. He also coins the term "metabolism" to describe the overall chemical changes that take place in living tissues.
- 1839 Invention of microfilm by John Dancer.
- 1840 Friedrich Gustav Jacob Henle publishes the first histology textbook, *General Anatomy*. This work includes the first modern discussion of the germ theory of communicable diseases.
- 1841 Eugene-Melchoir Peligot isolates the element uranium.
- 1843 Charles-Frédéric Gerhardt, French chemist, simplifies chemical formula-writing, so that water becomes H<sub>2</sub>O instead of the previous H<sub>4</sub>O<sub>2</sub>.
- 1843 Howard Aiken develops first mechanical programmable calculator.
- 1844 Samuel Morse sends the first message via telegraph. His code (Morse code) and telegraph were able to send messages over lines in a matter of minutes, requiring only knowledge of the operational code. As soon as governments began to use telegraphs to send vital communications, rival intelligence services learned to tap the line, gaining access to secret communications and conducting detailed surveillance from a comfortable distance. Use of the telegraph necessitated the development of complex codes and the creation of specialized cryptology departments. By the turn of the twentieth century, most national intelligence operations in Europe and the United States were involved communications surveillance and the tapping of both wired and wireless telegraphs.
- 1845 Christian Friedrich Schönbein, German-Swiss chemist, prepares guncotton. He discovers that a certain acid mixture combines with the cellulose in cotton to produce an explosive that burns without smoke or residue.
- 1846 Ascanio Sobrero, Italian chemist, slowly adds glycerin to a mixture of nitric and sulfuric acids and first produces nitroglycerine. He is so impressed by the explosive potential of a single drop in a heated test tube and so fearful of its use in war that he makes no attempt to exploit it. It is another 20 years before Alfred Nobel learns the proper formula and puts it to use.
- 1846 U.S. forces victorious in Mexican War, which results in annexation of what is today the southwestern United States.
- 1848 U.S. Congress passes Drug Importation Act that allows U.S. Customs Service inspection to stop entry of foreign drugs.
- 1849 First aerial bombardment campaign, by Austrians against Venetians, using 200 unpowered hot-air balloons containing bombs set on timers.
- 1852 Jean Foucault invents gyroscope, an important instrument still used in modern navigation and guidance systems.
- 1855 Henri-Etienne Sainte-Claire Deville, French chemist, first produces aluminum in a pure state. He produces the metal in quantity by heating aluminum chloride with metallic sodium.



- 1856** Second Opium War begins between Britain and China. The conflict lasts until 1860. Also known as the Arrow War, or the Anglo-French War in China, the war broke out after a British-flagged ship, the *Arrow*, is impounded by China. France joins Britain in the war after the murder of a French missionary. China is again defeated, resulting in another large indemnity and the legalization of opium under the Treaty of Tientsin.
- 1857** Louis Pasteur demonstrates that lactic acid fermentation is caused by a living organism. Between 1857 and 1880, he performs a series of experiments that refute the doctrine of spontaneous generation. He also introduces vaccines for fowl cholera, anthrax, and rabies, based on attenuated strains of viruses and bacteria.
- 1858** Charles Darwin and Alfred Russell Wallace agree to a joint presentation of their theory of evolution by natural selection.
- 1858** Rudolf Ludwig Carl Virchow publishes his landmark paper "Cellular Pathology" and establishes the field of cellular pathology. Virchow asserts that all cells arise from preexisting cells (*Omnis cellula e cellula*). He argues that the cell is the ultimate locus of all disease.
- 1858** A group of the Irish Republican Brotherhood (IRB) forms another revolutionary group, the Fenian Brotherhood, with the goal of freeing Ireland from British rule.
- 1861** U.S. Civil War (1861–1865). Morphine gains wide medical use during the conflict.
- 1861** President-elect Abraham Lincoln arrives secretly in Washington to foil assassination plot brewing in Baltimore.
- 1861** Balloonist and Ohioan Thaddeus Lowe is accused by irate South Carolina citizens of being a Yankee spy after his balloon lands following a 500 mile aerial flight. Lowe eventually volunteers his services to Union forces and becomes director of the Union's balloon corps. His resignation two years later brings the corps to an end.
- 1861** Rose O'Neal Greenhow is arrested as Confederate spy after warning General P.G.T. Beauregard of a planned Union attack on Manassas in July 1861. She is released in 1862 but dies in a shipwreck.
- 1862** Department of Agriculture establishes the Bureau of Chemistry, the organizational forerunner of the Food and Drug Administration.
- 1862** Legal Tender Act authorizes the U.S. government to issue currency notes through the Treasury Department. These notes, which Treasury continues to issue until 1971, are known as U.S. notes.
- 1862** In September, President Lincoln suspends the right of *habeas corpus* in order to allow federal authorities to arrest and detain suspected Confederate sympathizers and draft resisters without arrest warrants or speedy trials. The following year, Congress reaffirms the suspension in the *Habeas Corpus Act* of 1863.
- 1863** Ferdinand Reich, German mineralogist, and his assistant Hieronymus Theodor Richter examine zinc ore spectroscopically and discover the new, indigo-colored element iridium. It is used in the next century in the making of transistors.
- 1863** Geology plays decisive role in the Battle of Gettysburg as Union troops hold key high-ground positions.
- 1863** Belle Boyd, a Confederate spy, is released from prison in Washington.
- 1864** James Clerk Maxwell develops equations of electromagnetic wave propagation.
- 1864** First Geneva Convention addresses "the amelioration of the condition of the wounded on the field of battle," resulting in principles for protecting noncombatant personnel caring for the wounded. The convention also establishes the International Red Cross.
- 1865** An epidemic of rinderpest kills 500,000 cattle in Great Britain. Government inquiries into the outbreak pave the way for the development of contemporary theories of epidemiology and the germ theory of disease.
- 1865** Gregor Mendel presents his work on hybridization of peas to the Natural History Society of Brno, Moravia. The paper is published in the 1866 issue of the society's *Proceedings*. Mendel presents statistical evidence that hereditary factors are inherited from both parents in a series of papers on "Experiments on Plant Hybridization" published between 1866 and 1869. His experiments provide evidence of dominance, the laws of segregation, and independent assortment, although the work is generally ignored until 1900.
- 1865** U.S. Secret Service established to interdict counterfeit currency and its manufacturers.
- 1865** President Lincoln is shot in Washington, D.C., by John Wilkes Booth. Lincoln dies the next day; Andrew Johnson assumes the presidency.
- 1865** The Molly McGuires, a secret society of Irish miners, attacks coal-mine operators and owners for mistreatment of workers.
- 1867** Alfred Nobel, Swedish inventor, invents dynamite, a safer and more controllable version of nitroglycerine. He combines nitroglycerine with "kieselguhr," or earth containing silica, and discovers that it cannot be exploded without a detonating cap.
- 1867** Secret Service responsibilities broadened to include "detecting persons perpetrating frauds against the government."
- 1869** Dimitri Ivanovich Mendeleev, Russian chemist, and Julius Lothar Meyer, German chemist, independently put forth the Periodic Table of Elements, which arranges the elements in order of atomic weights. However, Meyer does not publish until 1870, nor does he predict the existence of undiscovered elements as Mendeleev does.
- 1870** Lambert Adolphe Jacques Quetelet shows the importance of statistical analysis for biologists and provides the foundations of biometry.
- 1870** Congress creates the Department of Justice.
- 1871** U.S. president Ulysses S. Grant establishes Office of the Surgeon General.

- 1872 Ferdinand Julius Cohn publishes the first of four papers entitled "Research on Bacteria," which establishes the foundation of bacteriology as a distinct field. He systematically divides bacteria into genera and species.
- 1873 James Clerk Maxwell, Scottish mathematician and physicist, publishes *Treatise on Electricity and Magnetism* in which he identifies light as an electromagnetic phenomenon. He determines this when he finds his mathematical calculations for the transmission speed of both electromagnetic and electrostatic waves are the same as the known speed of light. This landmark work brings together the three main fields of physics—electricity, magnetism, and light.
- 1876 German bacteriologist Robert Koch publishes a paper on anthrax that implicates a bacterium as the cause of the disease, validating the germ theory of disease.
- 1876 Alexander Graham Bell patents the telephone.
- 1876 The first microphone is invented by Emile Berliner.
- 1877 Congress passes legislation prohibiting the counterfeiting of any coin, gold, or silver bar.
- 1878 Charles-Emanuel Sedillot introduces the term "microbe." The term becomes widely used as a term for a pathogenic bacterium.
- 1878 In a backlash against 12 years of martial law in the southern United States, Congress passes the Posse Comitatus Act, which forbids the military from enforcing domestic law.
- 1880 First attempt at passage of a nationwide food and drug law. Although defeated in Congress, U.S. Department of Agriculture's findings of widespread food adulteration spur continued interest in food and drug legislation.
- 1880 Louis Pasteur develops a method of weakening a microbial pathogen of chicken, and uses the term "attenuated" to describe the weakened microbe.
- 1881 President James A. Garfield is shot on July 2, 1881, in Washington, D.C., by anarchist Charles J. Guiteau. Garfield dies on September 19; Chester A. Arthur assumes the presidency.
- 1882 Robert Koch discovers the tubercle bacillus and enunciates "Koch's postulates," which define the classic method of preserving, documenting, and studying bacteria.
- 1882 Establishment of the Office of Naval Intelligence, which by the early twenty-first century will be the oldest continually operating intelligence agency in the United States.
- 1883 George Francis Fitzgerald, Irish physicist, first suggests a method of producing radio waves. From his studies of radiation, he concludes that an oscillating current will produce electromagnetic waves. This is later verified experimentally by Hertz in 1888 and used in the development of wireless telegraphy.
- 1883 U.S. Secret Service is officially embodied as a distinct organization within the Treasury Department.
- 1883 British inventor Hiram Stevens Maxim invents the machine gun.
- 1884 Louis Pasteur and coworkers publish a paper titled "A New Communication on Rabies." Pasteur proves that the causal agent of rabies can be attenuated and the weakened virus can be used as a vaccine to prevent the disease. This work serves as the basis of future work on virus attenuation, vaccine development, and the concept that variation is an inherent characteristic of viruses.
- 1885 U.S. Army establishes its Division of Military Information, its formal military intelligence organization.
- 1887 Ernst Mach, Austrian physicist, is the first to note the sudden change in the nature of the airflow over a moving object that occurs as it approaches the speed of sound. Because of this, the speed of sound in air is called Mach 1. Mach 2 is twice that speed, and so on.
- 1888 Heinrich Rudolf Hertz, German physicist, for the first time generates electromagnetic (radio) waves and devises a detector that can measure their wavelength. From this he is able to prove experimentally James Clerk Maxwell's hypothesis that light is an electromagnetic phenomenon. Hertz's work not only discovers radio waves, but experimentally unites the three main fields of physics—electricity, magnetism, and light.
- 1889 Frederick Augustus Abel, English chemist, and James Dewar, Scottish chemist and physicist, invent cordite and pioneer the production of smokeless powder. Their new mixture borrows from previous discoveries but proves safer to handle.
- 1889 Johann Philipp Ludwig Julius Elster and Hans Friedrich Geitel, both German physicists, study the photoelectric effect (when an electric current is created upon the exposure of certain metals to light) and produce the first practical photoelectric cells that can measure the intensity of light.
- 1890 Oliver Joseph Lodge, English physicist, invents the coherer, a detector of radio waves that, although replaced, makes him one of the pioneers of early radio communication. He also suggests correctly that the sun emits radio waves.
- 1892 George M. Sternberg publishes his *Practical Results of Bacteriological Researches*. Sternberg's realization that a specific antibody was produced after infection with vaccinia virus and that immune serum could neutralize the virus becomes the basis of virus serology. The neutralization test provides a technique for diagnosing viral infections, measuring the immune response, distinguishing antigenic similarities and differences among viruses, and conducting retrospective epidemiological surveys.
- 1892 U.S. Congress awards Harriet Tubman a pension for her work as a Union nurse, spy and scout during the Civil War.
- 1894 U.S. Secret Service begins part-time protection of U.S. president Grover Cleveland.
- 1895 Wilhelm Conrad Röntgen, German physicist, discovers x rays. While working on cathode ray tubes and experimenting with luminescence, he notices that a

- nearby sheet of paper that is coated with a luminescent substance glows whenever the tube is turned on. For seven weeks he continues to experiment, and near the end of the year is able to report the basic properties of the unknown rays he names “x rays.”
- 1896** Antoine-Henri Becquerel, French physicist, discovers radioactivity in uranium ore.
- 1896** Guglielmo Marconi, Italian electrical engineer, travels to England to apply for and obtain the first patent in the history of radio. By this time, he has sent and received a radio signal over nine miles.
- 1896** Johann Elster and Hans Friedrich Geitel study the newly discovered radioactivity and demonstrate that external effects do not influence the intensity of radiation. They are also the first to characterize radioactivity as being caused by changes that occur within the atom.
- 1897** Joseph John Thomson, English physicist, discovers the electron. He conducts cathode ray experiments and concludes that the rays consist of negatively charged “electrons” that are smaller in mass than atoms.
- 1898** Marie Sklodowska Curie and Pierre Curie discover the radioactive element radium. They spend the next four years refining eight tons of pitchblende to obtain a full gram of radium.
- 1898** Spanish-American War.
- 1899** First Hague Conference establishes international laws of conduct in warfare.
- 1900** Carl Correns, Hugo de Vries, and Erich von Tschermak independently rediscover Mendel’s laws of inheritance. Their publications mark the beginning of modern genetics. Using several plant species, de Vries and Correns perform breeding experiments that parallel Mendel’s earlier studies and independently arrive at similar interpretations of their results. Therefore, upon reading Mendel’s publication, they immediately recognized its significance. William Bateson describes the importance of Mendel’s contribution in an address to the Royal Society of London.
- 1900** Ernest Rutherford, British physicist, first determines radioactive half-life.
- 1900** Friedrich Ernst Dorn, German physicist, demonstrates that radium emits a gas as it produces radioactivity. This proves to be the first evidence that in the radioactive process one element is actually transmuted into another.
- 1900** Karl Landsteiner discovers the blood-agglutination phenomenon and the four major blood types in humans.
- 1901** President William McKinley is assassinated by anarchist Leon Czolgosz.
- 1901** United States acquires rights from Cuba to use Guantanamo Bay indefinitely as a naval base.
- 1901** Antoine Henri Becquerel, French physicist, studies the rays emitted by the natural substance uranium and concludes that the only place they could be coming from is within the atoms of uranium. This marks the first clear understanding of the atom as something more than a featureless sphere. Becquerel’s discovery of radioactivity and his focus on the uranium atom make him the father of modern atomic and nuclear physics.
- 1901** After the assassination of President William McKinley, Congress formally places the U.S. Secret Service—which first began guarding presidents during the second Grover Cleveland administration seven years before—in charge of protecting the president.
- 1901** Henry Classification System devised for fingerprint analysis by Sir Edward Henry.
- 1902** The Secret Service assumes full-time responsibility for protection of the president. Two operatives are assigned full time to the White House detail.
- 1902** U.S. Congress passes Spooner Act, which authorizes the United States to purchase the assets of a French company that had attempted to build a canal through Panama, and to begin a U.S. effort toward building a canal.
- 1902** Oliver Heaviside, English physicist and electrical engineer, and Arthur Edwin Kennelly, British-American electrical engineer, independently and almost simultaneously make the first prediction of the existence of the ionosphere, an electrically conductive layer in the upper atmosphere that reflects radio waves. They theorize correctly that wireless telegraphy works over long distances because a conducting layer of atmosphere exists that allows radio waves to follow Earth’s curvature instead of traveling off into space.
- 1903** For their work in the physics of radioactivity, Antoine Becquerel, Pierre Curie, and Marie Curie are awarded the Nobel Prize for physics.
- 1903** Panama secedes from Colombia. The new government will cooperate in the building of the Panama Canal.
- 1903** U.S. Army implements the concept of a permanent general staff, and with it the idea, pioneered in Europe, of the four sections of a military command. The Division of Military Information thus becomes G-2.E170.
- 1903** Orville and Wilbur Wright make the first powered flight.
- 1904** Roosevelt Corollary to the Monroe Doctrine asserts that the United States has the right to assume the defacto role of an international police power.
- 1904** Congress creates Panama Canal Zone, and in the summer construction on the Panama Canal begins.
- 1905** Bloody Sunday incident in Russia. Tsarist troops fire on marchers in St. Petersburg.
- 1905** Sinn Fein political movement for Irish independence is founded.
- 1905** Albert Einstein, German-Swiss physicist, publishes his second paper on relativity including his famous equation stating the relationship between mass and energy:  $E = mc^2$ . In this equation, E is energy, m is

- mass, and  $c$  is the velocity of light. This contains the revolutionary concept that mass and energy are simply different aspects of the same phenomenon.
- 1906** Congress passes Sundry Civil Expenses Act, which provides funds for presidential protection by the Secret Service.
- 1906** Secret Service operatives began to investigate the western land frauds. The investigations return millions of acres of land to the government. Operative Joseph A. Walker is murdered on November 3, 1907, while working on one of these cases, becoming the first operative killed in the line of duty.
- 1907** Triple Entente formed as Great Britain formally joins the defense pact between France and Russia.
- 1907** Bertram Borden Boltwood, American chemist and physicist, discovers what he believes is a new element which he calls ionium. It is later determined to be a radioactive isotope of thorium. Boltwood also invents a radioactive dating procedure.
- 1907** Second Hague Conference establishes further international laws of conduct in warfare, with a focus on war in a maritime environment.
- 1907** Establishment of Aeronautical Section of the U.S. Army Signal Corps—first incarnation of the U.S. Air Force. This becomes the Aviation Section in 1914.
- 1908** Large deposits of petroleum are discovered in the Middle East.
- 1908** Ernest Rutherford and Hans Wilhelm Geiger develop an electrical alpha-particle counter. Over the next few years, Geiger continues to improve this device which becomes known as the Geiger counter.
- 1908** Secret Service begins protecting the president-elect.
- 1908** A Sundry Civil Service Bill declares that Secret Service employees accepting assignments by any department other than Treasury (except in counterfeiting cases) would be suspended for two years. The provision became effective July 1, and prevented the practice of agencies like the Department of Justice (DOJ) borrowing investigators for specific cases.
- 1908** Formal beginning of the Bureau of Investigation (BOI), which became the FBI in 1935.
- 1909** U.S. Congress passes Copyright Law.
- 1909** Alfred Stock, German chemist, first synthesizes boron hydrides (compounds of boron and hydrogen). Forty year later, boron hydrides prove useful to space exploration as additives to rocket fuel.
- 1909** An intelligence report in the British Parliament leads to the establishment of the Secret Service Bureau, precursor to both MI5 and MI6.
- 1910** The United States sends military forces to Mexico during Mexican revolution.
- 1910** Britain signs an agreement with China to dismantle the opium trade. However, the profits made from its cultivation, manufacture, and sale were so enormous that no serious interruption would be effected until World War II closed supply routes throughout Asia.
- 1910** Congress passes the White Slave Traffic Act on June 25. Also known as the Mann Act, this new law significantly increases BOI jurisdiction over interstate crime.
- 1911** At 11:01 a.m. on January 18, the U.S. Navy's Eugene Ely lands a Curtiss pusher aircraft on a specially built platform aboard the USS *Pennsylvania*. Thus is born the concept of the aircraft carrier.
- 1911** Fritz Pregl, Austrian chemist, first introduces organic microanalysis. He invents analytic methods that make it possible to determine the empirical formula of an organic compound from just a few milligrams of the substance.
- 1911** Heike Kamerlingh-Onnes, Dutch physicist, first discovers the phenomenon of superconductivity when he studies the properties of certain metals subjected to the low temperatures of liquid helium. He finds that some metals, like mercury and lead, undergo a total loss of electrical resistance. He also discovers that a form of liquid helium is produced which has properties unlike any other substances.
- 1911** Marie Curie receives the Nobel Prize in chemistry for the discovery of the elements radium and polonium, for the isolation of radium, and for investigating its compounds. It is Curie's second Nobel Prize.
- 1911** Georg von Hevesy conceives the idea of using radioactive tracers. Von Hevesy later wins the Nobel Prize in 1943.
- 1911** Italians make first use of aircraft in combat during 1911–12 war against Turkey. On October 23, Italians conduct first reconnaissance in an airplane, against Turkish troops near Tripoli in what is now Libya. On November 1, the Italians again make aviation history when they conduct the first aerial bombing raid against an enemy.
- 1912** U.S. Marines invade Honduras, Cuba, and Nicaragua to protect American interests. U.S. troops will remain in Nicaragua until 1930s.
- 1912** The U.S. Public Health Service is established.
- 1912** Joseph Thomson develops a forerunner of mass spectrometry and separation of isotopes.
- 1912** Max von Laue, German physicist, obtains diffraction pattern for x rays through a crystal and offers evidence that x rays are a form of electromagnetic radiation and are waves. This marks the beginning of studies on the physics of solids as an analysis of the periodic and regular disposition of atoms in a crystal.
- 1912** Paul Ehrlich discovers a chemical cure for syphilis. This is the first chemotherapeutic agent for a bacterial disease.
- 1912** Theodore Roosevelt survives assassination attempt on October 14 in Milwaukee while campaigning for a second term as president.
- 1913** U.S. troops assist in pursuit of Mexican rebel leader Francisco Pancho Villa in northern Mexico.
- 1913** Congress authorizes permanent protection of the president and the statutory authorization for president-elect protection.

- 1913 Harry Brearly, English metallurgist, accidentally discovers a nickel-chromium alloy that is corrosion resistant. It becomes stainless steel.
- 1913 Max Bodenstein, German physical chemist, develops the concept of a chain reaction in which one molecular change triggers another, and so on.
- 1913 U.S. Congress passes Federal Reserve Act, creating Federal Reserve System.
- 1913 Ratification of Sixteenth Amendment to the Constitution, which gives Congress power to levy taxes.
- 1914 The assassination of Austrian Archduke Francis Ferdinand precipitates World War I.
- 1914 World War I places additional responsibilities on the BOI. On April 6, 1917, Congress declares war on Germany and President Woodrow Wilson authorizes the BOI to detain enemy aliens.
- 1914 Panama Canal opens on August 15.
- 1915 Germany uses poison gas at the Battle of Ypres.
- 1915 A U-boat sinks the British ship *Lusitania*, a passenger ship also carrying military supplies from the United States to Britain.
- 1915 Frederick William Twort publishes the landmark paper *An Investigation of the Nature of Ultra-Microscopic Viruses*. Twort notes the degeneration of bacterial colonies and suggests that the causative agent is an ultra-microscopic-filterable virus that multiplies true to type.
- 1915 President Wilson directs the secretary of the treasury to have the Secret Service investigate espionage in the United States.
- 1915 U.S. Coast Guard founded.
- 1915 British nurse Edith Cavell is shot as a spy by a German firing squad for assisting British soldiers seeking to escape the Germans.
- 1915 After denouncing them as spies, the United States expels German attaches.
- 1916 German use of zeppelins, important both as surveillance craft and bombers during the first two years of World War I, begins to decline in September, after Allies develop special explosive bullets capable of downing airships.
- 1916 The Black Tom explosion. On July 29, German agents set fire to a complex of warehouses and ships in the New York harbor that hold munitions, fuel, and explosives bound to aid the Allies in their fight. Though the United States is technically a neutral nation at the time of the attack, their general policies greatly favor the Allies. The attack persuades many that the United States should join the Allies and intervene in the war in Europe.
- 1916 The Home Section of the British Secret Service Bureau becomes MI5, or the Security Service.
- 1916 Mexican guerrilla leader Pancho Villa conducts a raid on Columbus, New Mexico, killing 17 Americans.
- 1917 The British issue a declaration calling for a Jewish homeland in Palestine.
- 1917 Congress authorizes permanent protection of the president's immediate family and "threats" directed toward the president become a federal violation.
- 1917 Tsarist Russia's February Revolution begins with rioting and strikes in St. Petersburg. Alexander Kerensky ultimately assumes control of democratic socialist provisional government, exposes undercover agents of the Okhrana.
- 1917 British signal intelligence, having cracked the German cipher, intercepts a message from German foreign minister Arthur Zimmermann to the Mexican president, promising to return territories Mexico had lost to the United States in the Mexican War if Mexico will enter the war on Germany's side.
- 1917 Mata Hari (the pseudonym of Dutch dancer Margaretha Geertruida Zelle), who joined the German secret service in 1907, is executed by French firing squad. Mata Hari betrayed many military secrets that were gained from Allied officers who were on intimate terms with her.
- 1917 United States declares war on Germany.
- 1917 The U.S. Army creates the Cipher Bureau within the Military Intelligence Division.
- 1917 American engineer Gilbert S. Vernam develops the first significant automated encryption and decryption device when he brings together an electromagnetic ciphering machine with a teletypewriter.
- 1917 U.S. Congress passes the Espionage Act, criminalizing the disclosure of military, industrial, or government secrets related to national security. The act also prohibits antiwar activism and refusal of conscription, sparking controversy.
- 1917 V.I. Lenin returns from exile to Russia following Romanov abdication of the Russian throne. Lenin leads a Bolshevik revolution in November.
- 1918 German radio officer Fritz Nebel develops the ADFGX cipher.
- 1918 Russia signs the Brest-Litovsk treaty, ending Russian participation in World War I.
- 1918 Bolsheviks execute Tsar Nicholas II and his family.
- 1918 Major Joseph O. Mauborgne of the U.S. Army devises the one-time pad, whereby sender and receiver possess identical pads of cipher sheets that are used once and then destroyed—a virtually unbreakable system.
- 1918 German engineer Arthur Scherbius invents a three-rotor cipher machine, the Enigma.
- 1918 Germany's Kaiser Wilhelm II abdicates and World War I ends in Europe after 20 million casualties and six million deaths.
- 1918 U.S. president Wilson's fourteen-point peace proposal introduced.
- 1918 Sedition Act of 1918 amends Espionage and Sedition Acts to broaden the arrest powers granted to federal agents in apprehending and detaining individuals suspected of treason or antiwar activity.

- 1918 Socialist Party leader Eugene V. Debs is convicted and sentenced to a ten-year prison term under the Espionage Act for an antiwar speech he delivers in Canton, Ohio. Debs is later pardoned by President Warren G. Harding in December 1921.
- 1918 Hungary overthrows the Austro-Hungarian monarchy.
- 1918 An influenza epidemic spreads across Asia and war-ravaged Europe to the Americas. The epidemic eventually kills 20 million people, including 500,000 Americans.
- 1919 The Treaty of Versailles requires Germany, now under the Weimar Republic, to cede territory to France, Belgium, and Poland; relinquish its colonies; and pay extensive war reparations that will eventually cripple the German economy. The U.S. Senate refuses to ratify the treaty.
- 1919 U.S. House of Representatives refuses to seat socialist Victor Berger, a congressman elected from Wisconsin.
- 1919 U.S. fears increase after anarchist groups target government and business leaders with bombs in April and May; the terrorist wave culminates in a series of bombings in eight U.S. cities on June 2. Under the orders of Attorney General A. Mitchell Palmer, federal agents begin round-up of suspected communists and anarchists in November. The Palmer Raids, as they became known, last until March 1920 and result in the arrest of 6,000 suspects.
- 1919 Anarchists Emma Goldman and Alexander Berkman are deported by the United States to Russia.
- 1919 Establishment of British Government Code and Cypher School (GC&CS) in November.
- 1919 Congress passes the National Motor Vehicle Theft Act, also known as the Dyer Act, on October 28. This act authorizes the Bureau of Investigation to investigate auto thefts that cross state lines.
- 1920 The League of Nations first meets in Geneva.
- 1920 Bolshevik or anarchist terrorists accused of September 16 bombing on Wall St. in New York City which kills 35 people and injures hundreds more.
- 1920 Iraq is placed under British mandate.
- 1921 Except for six counties in Protestant Northern Ireland, the British Parliament grants Ireland dominion status.
- 1921 William Marston develops first modern polygraph.
- 1921 Twenty-six-year-old J. Edgar Hoover is named assistant director of BOI.
- 1922 Militants in the Irish Sinn Fein party form the Irish Republican Army (IRA).
- 1922 White House police force created at request of President Warren G. Harding. Ultimately this will become the uniformed division of the U.S. Secret Service.
- 1922 On March 20, U.S. Navy commissions the *Langley*, its first aircraft carrier. Later that year, the United States and other powers sign the Washington Naval Limitation Treaty, which controls battleship inventories, thus spurring carrier production. Congress authorizes the conversion of the unfinished battleships *Lexington* and *Saratoga* to become the navy's second and third carriers.
- 1922 Benito Mussolini becomes Italian dictator and forms a Fascist government.
- 1923 Union of Soviet Socialist Republics (U.S.S.R.) formed.
- 1923 Adolf Hitler, leader of the German Nazi party, attempts to seize power. He is arrested and sentenced to prison.
- 1923 Works published before 1923 are now in the public domain, meaning that they no longer hold a copyright, though a particular translation, made more recently, may be copyrighted. For works published after 1923, there are specific provisions as to when the item becomes part of the public domain. Some of these provisions, and other aspects of U.S. copyright law, are governed by the Berne Convention for the Protection of Literary and Artistic Works, which the United States signed in 1989.
- 1924 Lenin dies, to be succeeded by a triumvirate of leaders headed by Joseph Stalin.
- 1924 The U.S. Navy creates its first cryptanalytic group within the Code and Signal Section of the Office of Naval Communications.
- 1924 From prison, Adolf Hitler publishes *Mein Kampf*, in which he outlines the plan for the conquest of eastern Europe and the extermination of the Jews, which he will undertake as German leader less than a decade later.
- 1924 J. Edgar Hoover designated director of the BOI.
- 1924 BOI establishes an identification division after Congress authorizes "the exchange of identification records with officers of the cities, counties, and states."
- 1925 France begins construction of defensive Maginot Line against future German aggression. The line eventually proves useless as Hitler's troops bypass the line during their 1940 conquest of France.
- 1925 Johannes Hans Berger, German neurologist, records the first human electroencephalogram (EEG).
- 1925 Patrick Blackett, English physicist, takes the first photographs of a nuclear reaction in progress. To achieve this he uses a Wilson cloud chamber and takes over 20,000 photographs of more than 400,000 alpha particle tracks and observes eight actual collisions of an alpha particle and a nitrogen molecule.
- 1925 Special Agent Edwin C. Shanahan becomes the first BOI agent killed in the line of duty.
- 1926 Jiang Jie-shi (Chiang Kai-shek) assumes control of the Chinese government.
- 1926 The passage of the Air Commerce Act creates the earliest predecessor of the FAA, called the Aeronautics Branch.
- 1926 U.S. Army Air Service becomes Army Air Corps.
- 1926 Emperor Showa Tenno Hirohito assumes power in Japan.

- 1926 U.S. forces intervene in Nicaragua against leftist nationalist insurgency led by Augusto Cesar Sandino.
- 1927 Jiang Jie-shi defeats Communist Mao Zedong's (Mao Tse-tung) "Autumn Harvest" rebellion.
- 1927 Charles Lindbergh makes first nonstop solo transatlantic flight.
- 1927 German physicist Werner Heisenberg publishes uncertainty principle.
- 1928 George Gamow, Russian-American physicist, develops the quantum theory of radioactivity which is the first theory to successfully explain the behavior of radioactive elements, some of which decay in seconds and others after thousands of years.
- 1928 Hermann Weyl, German mathematician, publishes his *Gruppen theorie und Quatenmechanik* in which he shows that most of the regularities of quantum phenomena on the atomic level can be most simply understood using group theory. His book helps mold modern quantum theory.
- 1928 Sixty-two nations sign the Kellogg-Briand Pact (including the United States, Great Britain, Japan, and Italy) and renounce war as a means to solve international disputes.
- 1929 Kingdom of Serbs, Croats, and Slovenes becomes Yugoslavia.
- 1929 Scottish biochemist Alexander Fleming discovers penicillin. He observes that the mold *Penicillium notatum* inhibits the growth of some bacteria. This is the first antibiotic, and it opens a new era of "wonder drugs" to combat infection and disease.
- 1929 John Douglas Cockcroft, English physicist, and Irish physicist Ernest Thomas Sinton Walton devise the first particle accelerator, which produces proton beam energies up to 600,000 volts. Three years later, they will use the accelerator to bombard lithium and produce two alpha particles (having combined lithium and hydrogen to produce helium). This is the first nuclear reaction that has been brought about through the use of artificially accelerated particles and without the use of any form of natural radioactivity; it will prove highly significant to the creation of an atomic bomb.
- 1929 Julius Arthur Nieuwland, Belgian-American chemist, develops neoprene, the first successful synthetic rubber.
- 1929 U.S. stock market crash in October ushers in Great Depression.
- 1930 U.S. Food, Drug, and Insecticide Administration is renamed Food and Drug Administration (FDA).
- 1930 Nils Edlefsen constructs the first cyclotron under the direction of the American physicist Ernest Orlando Lawrence. This first instrument is a small machine that is used to produce directed beams of charged particles. Over the next few years, Lawrence continues to build larger instruments, which eventually contribute to the discovery of new elements.
- 1930 U.S. Treasury Department creates Bureau of Narcotics, which will remain the principal anti-drug agency of the federal government until the late 1960s.
- 1930 Establishment of U.S. Army Signal Intelligence Service (SIS) to consolidate all military operations in cryptography and cryptanalysis.
- 1930 Primitive anthrax vaccine developed.
- 1931 Japanese invade Manchuria.
- 1932 James Chadwick, English physicist, proves the existence of the neutral particle of the atom's nucleus, called the neutron. It proves to be by far the most useful particle for initiating nuclear reactions.
- 1932 Werner Heisenberg wins the Nobel Prize in physics for the creation of quantum mechanics, which has led to the discovery of the allotropic forms of hydrogen.
- 1932 Aldous Huxley publishes the novel *Brave New World*, which presents a dystopian view of genetic manipulations of human beings.
- 1932 The BOI starts the international exchange of fingerprint data with friendly foreign governments. Later halted as war approached, the program was not reinstated until after World War II.
- 1932 In response to the Lindbergh kidnapping case and other high-profile cases, the Federal Kidnapping Act is passed to authorize BOI to investigate kidnappings perpetrated across state borders.
- 1932 Iraq declared an independent state.
- 1932 BOI establishes technical laboratory.
- 1933 In January, Adolf Hitler and Nazi Party take power in Germany. By the end of the year, Hitler proclaims Third Reich.
- 1933 U.S. president-elect Franklin D. Roosevelt escapes assassination attempt in Miami.
- 1933 Gilbert Newton Lewis, American chemist, is the first to prepare a sample of water in which all the hydrogen atoms consist of deuterium (the heavy hydrogen isotope). Called "heavy water," this will later play an important role in the production of the atomic bomb.
- 1934 Frédéric Joliot-Curie and Irène Joliot-Curie, a husband-and-wife team of French physicists, discover what they call *artificial radioactivity*. They bombard aluminum to produce a radioactive form of phosphorus. They soon learn that radioactivity is not confined only to heavy elements like uranium, but that any element can become radioactive if the proper isotope is prepared. For producing the first artificial radioactive element they win the Nobel Prize in chemistry the next year.
- 1934 John Marrack begins a series of studies that leads to the formation of the hypothesis governing the association between an antigen and the corresponding antibody.
- 1934 In an attempt to reduce organized crime violence, the U.S. Congress passes the National Firearms Act, which places restrictions on the sale of certain weapons favored by gang members.
- 1935 German Nazi party formalizes anti-Semitism with passage of Nuremberg laws.

- 1935 In violation of the Versailles Treaty, Germany begins to rearm and reconstitutes the German Air Force (Luftwaffe).
- 1935 Federal Bureau of Narcotics, forerunner of the modern Drug Enforcement Administration (DEA), begins a campaign portraying marijuana as a drug that leads to addiction, violence, and insanity. The government produces films such as *Marihuana* (1935), *Reefer Madness* (1936), and *Assassin of Youth* (1937).
- 1935 Irish Protestants in Belfast riot against Catholics, provoking Catholic retaliation.
- 1935 Patrick Maynard Stuart Blackett, English physicist, demonstrates that when gamma rays pass through lead, they sometimes disappear and give rise to a positron and an electron. This is the first demonstrable case of the conversion of energy into matter and as such, is a confirmation of Einstein's famous  $E=mc^2$  equation.
- 1935 Robert Watson-Watt develops design for RADAR.
- 1935 Italian forces invade Ethiopia. The League of Nations, formed after World War I as an international body to ensure stability, fails to act.
- 1935 The BOI officially becomes the Federal Bureau of Investigation (FBI) on July 1.
- 1936 Spanish Civil War begins and becomes an international battleground pitting Francisco Franco's Fascist right against Marxist republican forces. Germany and Italy support Franco, while Soviet Union backs republicans. War will end with Franco's victory in 1939.
- 1936 Joseph Stalin begins a "great purge." Lysenkoism, a repressive pseudoscientific set of beliefs, also begins to gain strength in Soviet politics.
- 1936 Sulphonamides, a class of antibiotics, introduced.
- 1936 Adolf Hitler includes synthetic fuel production as a priority in his Four-Year Plan.
- 1936 Eugene Paul Wigner, Hungarian-American physicist, proposes the theory of neutron absorption which comes into play when nuclear reactors are built.
- 1936 Germany reoccupies the Rhine River area, a key move toward later expansion in Europe.
- 1936 Italy and Germany sign Axis Pact, to which Japan will become a signatory in 1940.
- 1936 President Roosevelt asks FBI to report on the activities of Nazi and communist groups.
- 1937 Italy withdraws from the League of Nations to join a Germany-Japan pact.
- 1937 Emilio Segre, Italian-American physicist, and Carlo Perrier bombard molybdenum with deuterons and neutrons to produce element 43, technetium. This is the first element to be prepared artificially that does not exist in nature.
- 1937 William Thomas Astbury, English physicist, first obtains information about the structure of nucleic acids by means of x-ray diffraction.
- 1937 Japan invades eastern China.
- 1938 German Nazis attack Jews and Jewish businesses during night of violence termed *Kristallnacht*.
- 1938 Hitler annexes Austria.
- 1938 At Munich conference in September, Germany, backed by Italy, gains title to the Sudetenland in western Czechoslovakia. Britain, led by Prime Minister Neville Chamberlain, and France, comply in this act of diplomatic conquest. After appeasing Hitler, Chamberlain returns to Britain and proclaims, "Peace in our time!"
- 1938 Otto Frisch and Lise Meitner advance theory of uranium fission.
- 1938 Swiss chemist Albert Hofmann at Sandoz Laboratories synthesizes LSD. After initial testing on animals, Hoffman's subsequent accidental ingestion of the drug in 1943 reveals LSD's hallucinogenic properties.
- 1938 German scientists develop sarin while researching pesticides.
- 1938 The House Un-American Activities Committee (HUAC; sometimes called the Dies Committee) is initially charged with ferreting out Nazi activity in the United States but also begins to attempt to investigate Communist activity.
- 1938 Orson Welles' radio drama based on H.G. Wells' novel *War of the Worlds* causes panic among listeners who believe Martians have invaded Earth.
- 1938 Debut of the Minox camera, designed by Walter Zapp of Latvia, which was destined to become one of the most widely used miniature cameras by intelligence services on both sides of the iron curtain.
- 1939 In Vietnam, Ho Chi Minh creates the Viet Minh party to oppose French colonialism.
- 1939 Ernest Chain and H.W. Florey refine the purification of penicillin, allowing the mass production of the antibiotic.
- 1939 President Roosevelt assigns responsibility for investigating espionage, sabotage and other subversive activities jointly to the FBI, the Military Intelligence Service of the War Department (MID), and the Office of Naval Intelligence (ONI).
- 1939 Leo Szilard, Hungarian-American physicist, and Canadian-American physicist Walter Henry Zinn confirm that fission reactions (nuclear chain reactions) can be self-sustaining using uranium.
- 1939 Marguerite Perey, French chemist, first isolates element number 87 from among the breakdown products of uranium. She names it francium, after her country.
- 1939 Niels Bohr, Danish physicist, proposes liquid-drop model of the atomic nucleus and offers his theory of the mechanism of fission. His prediction that it is the uranium-235 isotope that undergoes fission is proved correct when work on an atomic bomb begins in the United States.
- 1939 Otto Hahn and Fritz Strassman publish results in which they observe that fission reactions can be self-sustaining because of the chain reaction that occurs.



- This discovery eventually makes the construction of an atomic bomb feasible.
- 1939 Paul Hermann Müller, Swiss chemist, discovers the insect-killing properties of DDT (dichlorodiphenyltrichloroethane). It is used during WW II to kill disease-carrying lice, fleas, and mosquitoes, and after the war to kill agricultural pests. It is later proved to be a harmful environmental pollutant and its use in the United States is banned in 1972.
- 1939 Richard Brooke Roberts, American biophysicist, discovers that uranium fission does not release all the neutrons it produces at one time. This phenomenon of *delayed neutrons* eventually proves to be an important element in the safety of nuclear reactors.
- 1939 U.S. Geological Survey strategic mineral program started.
- 1939 The little-known tank battle at Nomonhan in August discourages Japanese hopes of easy victory against Soviets—a major factor motivating the Japanese refusal to join Germans in attacking Soviet Union two years later.
- 1939 Nazi Germany and Soviet Union sign Non-Aggression Pact on August 23.
- 1939 Albert Einstein sends a letter to President Roosevelt informing him of German atomic research and the potential for the development of an atomic bomb.
- 1939 World War II begins with the German invasion of Poland on September 1. Britain and France declare war on Germany.
- 1940 Germany launches a full-scale air war against England and extends persecution of the Jews into Poland, Romania, and the Netherlands.
- 1940 Winston Churchill succeeds Neville Chamberlain as Britain's prime minister.
- 1940 Ernest Chain and E.P. Abraham detail the inactivation of penicillin by a substance produced by *Escherichia coli*. This is the first bacterial compound known to produce resistance to an antibacterial agent.
- 1940 Leon Trotsky is assassinated in Mexico City by agents of SMERSH (*SMERrt SHpionam* or "Death to Spies").
- 1940 The British begin to intercept German non-Morse teleprinter text that used the Baudot Code, an international standard where each letter is represented by five binary elements.
- 1940 The FBI participates in the growing Red Scare by conducting additional arrests of suspected Communist agents under powers granted by the 1940 Smith Act, which permits the arrest of any individual inciting the overthrow of the government.
- 1940 The FBI establishes a Special Intelligence Service (SIS).
- 1941 The Lend-Lease Act allows the United States to send military supplies to Britain and other allies.
- 1941 Arnold O. Beckman, American physicist and inventor, invents the spectrophotometer. This instrument measures light at the electron level and can be used for many kinds of chemical analysis.
- 1941 Glenn Theodore Seaborg, American physicist, and his colleagues prepare the transuranium element 94, plutonium.
- 1941 Fairbairn-Sykes fighting knife first produced and used by Allies in World War II.
- 1941 U.S. Army Air Corps becomes Army Air Force. Six years later, the National Security Act of 1947 will transform this group into a full military service, the U.S. Air Force.
- 1941 On June 22, Germany launches largest land invasion in history against Soviet Union. Initial German efforts will meet with success, but three Russian winters, combined with Russian resistance, will result in German defeat by early 1944.
- 1941 U.S. president Roosevelt appoints William J. (Wild Bill) Donovan as Coordinator of Information, a proto intelligence service.
- 1941 On December 7, the Japanese attack the U.S. naval base at Pearl Harbor, Hawaii. In response, the United States enters World War II. The FBI is authorized to act against dangerous enemy aliens and to seize enemy aliens and contraband (e.g. short-wave radios, dynamite, weapons, and ammunition).
- 1942 German Nazi party makes Jewish extermination a systematic state policy, termed the "Final Solution."
- 1942 In the United States, economic depression is relieved by war production of planes, tanks, and other military supplies.
- 1942 The largest detainment of American citizens in the name of national security (ultimately resulting in the internment of 110,000 Japanese-Americans during World War II) begins two months after the Japanese attack on Pearl Harbor. The U.S. Department of Justice orders the detention of about 2,200 Japanese, 1,400 German, and 269 Italian nationals. More than 47,000 Issei (Japanese-born residents) are barred under federal law from gaining American citizenship, and 80,000 of their American-born family members, called Nissei, are subject to internment under Executive Order 9066, signed by President Roosevelt in February.
- 1942 Despite early losses in the war, Allied forces rally, defeating German Field Marshal Erwin Rommel in North Africa.
- 1942 Office of Strategic Services formed by President Roosevelt and led by William J. Donovan.
- 1942 Alcohol Tax Unit (ATU) formed and given responsibility for enforcing the Firearms Act.
- 1942 The U.S. military creates the Army-Navy Communications Intelligence Board (ANCIB).
- 1942 The Manhattan Project is formed to secretly build the atomic bomb before the Germans.
- 1942 Enrico Fermi, Italian-American physicist, heads a Manhattan Project team at the University of Chicago that produces the first controlled chain reaction in an atomic pile of uranium and graphite. With this first self-sustaining chain reaction, the atomic age begins.

- 1942 Frank Harold Spedding, American physicist, develops the necessary methods to produce pure uranium in very large quantities for the U.S. atomic bomb effort. Spedding's laboratory produces two tons in November, to be used for the first "atomic pile."
- 1942 The Clinton Engineer Works is built in Oak Ridge, Tennessee (later renamed the Oak Ridge National Laboratory). The Clinton Pile, the first true plutonium production reactor, begins operation in November 1943.
- 1942 Harvard University chemist Louis F. Fieser invents napalm.
- 1942 U.S. Geological Survey establishes military geology branch.
- 1942 Selman Waksman suggests that the word "antibiotics" be used to identify antimicrobial compounds that are made by bacteria.
- 1942 British Government Code and Cypher School (GC&CS) renamed the Government Communications Headquarters (GCHQ) to conceal its cryptologic mission.
- 1942 U.S. Naval intelligence breaks the Japanese navy's JN-25 code, providing valuable intelligence from the Battle of Midway to the end of World War II.
- 1942 U.S. naval victories against Japan in the naval battles of the Coral Sea in May and Midway in June. Fought primarily with carriers and aircraft, the first of these marks history's first naval battle in which opposing fleets' ships never came in sight of one another.
- 1942 Four German saboteurs come ashore from a U-boat on the beach near Amagansett, Long Island. Within the week, a second team of German saboteurs lands in Florida. Some saboteurs surrender and within two weeks the FBI captures the others.
- 1943 Mussolini overthrown and arrested on July 25; Prime Minister Pietro Badoglio, who has secretly been in contact with Allies, becomes Italian leader. Italy surrenders to the Allies. Mussolini is later rescued in a daring German airborne raid on September 12. He will spend the remainder of the war (and his life) as head of a puppet government based in the northern Italian town of Salo.
- 1943 The Soviet army defeats German troops at Stalingrad.
- 1943 Stalin abolishes the Soviet Comintern and the KGB and GRU (Soviet Army Intelligence) assume all espionage activities.
- 1943 J. Robert Oppenheimer, American physicist, is placed in charge of U.S. atomic bomb production at Los Alamos, New Mexico. He supervises the work of 4,500 scientists and oversees the successful design construction and explosion of the bomb.
- 1943 Lars Onsager, Norwegian-American chemist, works out the theoretical basis for the gaseous-diffusion method of separating uranium-235 from the more common uranium-238. This is essential for producing a nuclear bomb or nuclear power.
- 1943 First operational nuclear reactor is activated at the Oak Ridge National Laboratory in Oak Ridge, Tennessee.
- 1943 Construction starts (completed 1945) at the Hanford Site in Richland, Washington, where plutonium is to be produced.
- 1943 Colossus Mark I, the world's first programmable computing machine, built.
- 1943 Lockheed establishes its advanced development programs headquarters at Palmdale, California. Over the years that follow, this facility, known as the "Skunk Works," will be the birthplace of extraordinary aircraft such as the U-2, the SR-71, and the F-117A.
- 1943 U.S. Army renames SIS as the Signal Security Agency, or SSA.
- 1943 The SZ43 cipher machine is first used by Germany in WWII. The German military did not replace Enigma with the SZ42 for general use because the SZ42's complexity made it too heavy for the field.
- 1943 On January 15, just 16 months after the September 11, 1941, groundbreaking, the new Pentagon building is dedicated in Washington, D.C.
- 1943 U.S. Army's Signal Intelligence Service, a forerunner of NSA, formally begins program codenamed VENONA to break encrypted Soviet diplomatic communications.
- 1943 Amy Elizabeth Thorpe, a U.S. born British spy known as "Cynthia" acts as World War II's "Mata Hari."
- 1944 To combat battle fatigue during World War II, nearly 200 million amphetamine tablets are issued to U.S. soldiers stationed in Great Britain during the war.
- 1944 Massive Allied invasion of European continent at Normandy in France on June 6 (D Day). Invasion, under the command of General Dwight D. Eisenhower, is preceded by deception effort designed to convince Germans that the action will occur elsewhere.
- 1944 Allies liberate France, allow French troops under de Gaulle to ceremonially enter Paris first. Nazi puppet government at Vichy, France, collapses.
- 1944 Assassination attempt on Hitler and several other high-ranking officials. Himmler suspects that the plot was the work of agents inside of the government, most especially the Abwehr.
- 1944 Colossus II computer becomes operational.
- 1944 Otto Hahn receives the Nobel Prize in chemistry for his discovery of nuclear fission.
- 1944 Soviet Viktor Kravchenko defects to United States.
- 1944 Stalin orders creation of Department S, which will use American scientists as Russian spies.
- 1944 Britain's MI6 establishes a section devoted to Soviet espionage and subversion. Unfortunately, its director is Harold (Kim) Philby, a Soviet agent.
- 1945 Yalta Summit sets forth terms of a divided postwar Europe.
- 1945 U.S. troops liberate Nazi concentration camp at Buchenwald.
- 1945 Italian dictator Benito Mussolini killed by partisans on April 28, Adolf Hitler commits suicide April 30, and

- Germany surrenders to the Allies on May 7. Germany is divided and occupied by the United States, the Soviet Union, Great Britain, and France.
- 1945 First atomic bomb is detonated by the United States at Trinity test site near Alamogordo, New Mexico. The experimental bomb generates an explosive power equivalent to 15–20 thousand tons of TNT. The United States then destroys the Japanese city of Hiroshima with a nuclear fission bomb based on uranium-235 on August 6. Three days later a plutonium-based bomb destroys the city of Nagasaki. Japan surrenders on August 14 and World War II ends. This is the first use of nuclear power as a weapon.
- 1945 U.S. Department of State intelligence experts join Army-Navy Communications Intelligence Board (ANCIB) to form combined State-Army-Navy Communications Intelligence Board (STANCIB).
- 1945 United States develops a radar-absorbent paint containing iron.
- 1945 Army Security Agency (ASA) begins to provide the U.S. Army with signal intelligence and security information (ASA operates until 1976).
- 1945 OSS is abolished; operations transfer to its successor, Central Intelligence Group (CIG).
- 1945 League of Arab States formed; United Nations (UN) is created on October 24.
- 1946 In a January 22 presidential directive, President Harry S. Truman first uses the term “Director of Central Intelligence” (DCI) which he designates as the lead position in the CIG within the National Intelligence Authority (NIA). NIA will be abolished, and the DCI will eventually lead the Central Intelligence Agency (CIA).
- 1946 U.S. diplomat George Kennan’s “Long Telegram” provides the ideological foundation for postwar policy toward the Soviet Union. Referring to the repressive Soviet domination of the Eastern Bloc states, British former prime minister Winston Churchill states that an “iron curtain” has come down across Europe.
- 1946 The organizational structure of the Royal Canadian Mounted Police is changed in response to the increased need for national security in Canada. Personnel are assigned to the Special Branch, which deals specifically with issues of national security.
- 1946 State-Army-Navy Communications Intelligence Board (STANCIB) becomes the U.S. Communications Intelligence Board (USCIB). FBI intelligence officers join the working group.
- 1946 In a postwar reorganization of the U.S. Army, the Military Intelligence Division is placed over the Army Security Agency and the Counter Intelligence Corps.
- 1946 U.S. Air Force Strategic Air Command (SAC) established at Offutt Air Force Base in Nebraska. It eventually becomes the command center for the defense “triad”: the strategic bombers and ICBMs (intercontinental ballistic missiles) of the Air Force, and the U.S. Navy’s submarine-launched ballistic missiles.
- 1946 On March 5, United States and United Kingdom sign UKUSA agreement, which brings together signals intelligence efforts of U.S., British, Canadian, Australian, and New Zealand agencies.
- 1946 American Electronic Numerical Integrator and Computer (ENIAC), is completed by the U.S. Army. ENIAC is considered the world’s first computer until information on Colossus was finally declassified in the 1970s.
- 1946 Establishment of Bureau of Intelligence & Research, intelligence arm of U.S. State Department.
- 1946 U.S. Army School of the Americas established in Panama.
- 1946 Baruch Plan for international control of atomic weapons presented to the UN.
- 1946 The United States tests a nuclear bomb on Bikini Atoll, an island in the Pacific.
- 1946 In August, Congress passes the Atomic Energy Act, creating Atomic Energy Commission, and makes FBI responsible for investigating persons having access to restricted nuclear data. The FBI will also be responsible for investigation of criminal violations of this act.
- 1946 First Vietnam war, between Viet Minh and France, begins December 19.
- 1947 Voice of America begins regular radio broadcasts to Russia from transmitters in Munich, Manila, and Honolulu in February.
- 1947 William Shockley, John Bardeen, and Walter Brattain invent the transistor.
- 1947 Vice-President Richard Nixon speaks in Congress, attacking Gerhart Eisler, who had been revealed as a German communist spy and who was then being detained on Ellis Island for passport fraud and refusing to testify before HUAC. The House agrees with Nixon and votes a contempt charge, but Gerhart escapes to East Germany as a stowaway.
- 1947 The Taft-Hartley Act of 1947 bans members of the Communist Party from holding leadership positions in American labor unions.
- 1947 Three “pillars” of the containment policy are in place: Truman Doctrine (March 12), Marshall Plan (June 5), National Security Act (July 28). Supporting instruments include DOD, CIA, SAC, advance bases in Turkey and Libya. Stalin creates the Cominform, or Information Bureau of Communist parties, in August, at the meeting in Poland of the Soviet, East European, French and Italian communist parties. Andrei Zhadov reports to the conference that America and Russia are locked in a two-camp struggle for world domination.
- 1947 Major Charles E. “Chuck” Yeager breaks the sound barrier in a Bell XS-1 rocket-powered research plane in October.
- 1947 HUAC subpoenas 41 witnesses in an investigation of communism in Hollywood films. Ten witnesses who refuse to testify are jailed for contempt; supporters sign an *amici curiae* Supreme Court brief and many are subsequently refused work in the film industry.
- 1947 The UN proposes a division of what is now Israel almost equally between Israelis and Arabs. Arab countries reject this proposal.

- 1947 On December 19, the National Security Council gives the CIA orders to conduct its first covert operation, influencing the general elections in Italy to prevent a Communist victory. The operation is successful, resulting in victory for the Christian Democrat party in 1948.
- 1948 Soon after Israel becomes a state in May, it is attacked by Egypt, Iraq, Jordan, and Syria. Though outnumbered, the Israelis defeat the Arab nations, and Israeli territory expands to encompass an area larger than that allotted in the original UN partition.
- 1948 NSC directive creates Office of Policy Coordination to conduct covert operations for the CIA. Former Wehrmacht officer Reinhard Gehlen is recruited to carry out espionage against Russia in Eastern Europe. Gehlen warns the CIA about the coming blockade of Berlin but is ignored.
- 1948 The United States organizes the Berlin airlift to break the blockade of Berlin (entirely within the Soviet sector of Germany) imposed by Soviets.
- 1948 Czech Foreign Minister Jan Masaryk is killed in a "fall" from his office window following a communist coup on February 25.
- 1948 Yugoslavia expelled from the Cominform.
- 1948 DPRK (North Korea) established.
- 1948 Executive Order 9835 establishes Federal Employee Loyalty Program. FBI begins background investigations and refers questionable cases to loyalty boards. Federal employees are subject to dismissal for specific acts including disclosure of confidential information and association with subversive organizations.
- 1948 Congress creates the Air Force Office of Special Investigations.
- 1948 Nuclear tests in the South Pacific (Operation Sandstone) pave the way for mass production of weapons that previously had to be assembled by hand. By late 1948, the United States has 50 nuclear bombs.
- 1948 Indictments issued against leaders of the U.S. Communist Party for violation of Smith Act (advocating violent overthrow of the government).
- 1948 Germanium crystals are used by the Bell Telephone Company in the United States to build the first transistors.
- 1948 World Health Organization (WHO) formed. The WHO subsequently becomes the principal international organization managing public health related issues on a global scale. Headquartered in Geneva, the WHO will eventually become an organization of more than 190 member countries, contributing to international public health in areas including disease prevention and control, promotion of good health, vaccination programs, and development of treatment and prevention standards.
- 1948 Alger Hiss testifies that he has never been a communist, never participated in espionage, and does not know Whittaker Chambers. Chambers, a former communist and editor for *Time* magazine previously testified to the HUAC that Hiss had once supplied him with stolen documents. Chambers then produced microfilm of secret documents hidden inside a pumpkin on his Maryland farm. Hiss is indicted on charges of perjury. Eventually he is convicted and serves a prison sentence.
- 1949 Victory of Mao Zedong in China forces Nationalist government to flee to Formosa, where it establishes the Republic of China. Meanwhile, the world's largest population falls under communist rule as the People's Republic of China.
- 1949 FDA publishes "black book" guide to toxicity of chemicals in food.
- 1949 Armed Forces Security Agency established to coordinate military communications intelligence and security activities.
- 1949 Federal Republic of Germany (West Germany) and German Democratic Republic (East Germany) are established.
- 1949 In April, ten countries (Belgium, Canada, Denmark, France, Iceland, Italy, Luxembourg, the Netherlands, Norway, Portugal) join the United States and the United Kingdom to form the North Atlantic Treaty Organization (NATO).
- 1949 Judith Coplon becomes the first U.S. citizen convicted as a spy, a conviction that was later reversed because of illegal FBI wiretaps.
- 1949 May 12, the Soviets finally lift the blockade on Berlin. Train and auto transport resumes into the city. Allied Airlift operations continue through September until supplies regularly reach Berlin via train and truck.
- 1949 The Central Intelligence Agency Act of 1949 provides special administrative authorities and responsibilities for the agency and the director.
- 1949 Russia announces that its first A-bomb was successfully tested July 14.
- 1949 The CIA-sponsored Radio Free Europe begins broadcasting to Soviet-controlled Eastern Europe.
- 1950 Puerto Rican nationalists attempt to assassinate President Truman. As a result of this incident, in which a Secret Service agent is killed, Congress greatly expands the duties of the Secret Service.
- 1950 President Truman orders the Atomic Energy Commission to begin work to develop the hydrogen bomb (H-bomb).
- 1950 Wisconsin senator Joseph McCarthy launches an effort to identify and eliminate communism in America. "McCarthyism" is used to describe McCarthy's tactics of public denunciation without proof and forcing testimony through intimidation.
- 1950 British security agents in February arrest Los Alamos physicist Klaus Fuchs after an investigation based on an FBI tip derived from Soviet telegrams decrypted and decoded by the Army Signals Agency with FBI investigative assistance.
- 1950 East German government, with the assistance of the Soviet intelligence community, establishes the Stasi.
- 1950 The FBI initiates the Ten Most Wanted Fugitives Program in May in order to draw national attention to dangerous criminals who have avoided capture.

- 1950 McCarran Internal Security Act enacted, mandating that all communist organizations must register with the attorney general. The act also prohibits communists from working in national defense and prevents those who are members of "totalitarian" organizations from entering the United States.
- 1950 North Korea invades South Korea, igniting the Korean War. U.S. military troops sent to expel North Korean forces as part of a UN coalition.
- 1950 Determined to create a framework and mechanism for the production of reliable intelligence estimates, General Walter Bedell Smith, when he becomes Director of Central Intelligence in October, institutes the concept and practice of developing national intelligence estimates.
- 1950 Arrest of Julius and Ethel Rosenberg, who are tried, convicted, and later executed for espionage against the United States.
- 1950 MacArthur crosses the 38th parallel in an attempt to liberate North Korea.
- 1950 President Truman escapes assassination attempt unhurt as two Puerto Rican nationalists shoot their way into Blair House in Washington, D.C. Officer Leslie Coffelt, of the White House police, is shot and killed. In response, Congress enacts legislation the following year that permanently authorizes Secret Service protection of the president, his immediate family, the president-elect, and the vice president.
- 1950 North Korean troops gain easy victories against UN forces, but when MacArthur launches a bold offensive at Inchon, he cuts the North Korean army in half. By Thanksgiving, he promises that U.S. troops will be home by Christmas, but on November 25, China enters the war, and drives the UN forces back to the 38th parallel. Allied bombing ensures that this line remains the boundary between North and South Korea.
- 1951 In *Dennis v. U.S.*, the Supreme Court upholds decisions declaring U.S. Communist Party illegal because the party constitutes a "clear and present danger." The Court reverses itself in 1957.
- 1951 The United States forms a special committee to analyze the nation's intelligence and cryptographic efforts. The committee is, in part, composed of the secretaries of state, defense, and the DCI (CIA director). Later in the year, President Truman issues a top-secret directive creating the National Security Agency (NSA).
- 1951 Mossad, Israel's chief intelligence collection, counterterrorism, and covert action agency, established on April 1.
- 1951 CIA is given responsibility to determine the overall requirements of foreign economic intelligence.
- 1951 General MacArthur, eager for victory against the Chinese in Korea, attempts to defy President Truman's orders to stand down, and calls for American citizens' support of his plan to invade China. For this act of insubordination, Truman relieves him of duty on April 11, and replaces him with General Matthew B. Ridgway.
- 1951 The first usable electricity from nuclear fission is produced.
- 1952 British scientists develop VX nerve agent while studying insecticides.
- 1952 First thermo-nuclear device is exploded successfully by the United States at the Eniwetok Atoll in the South Pacific. This hydrogen-fusion bomb (H bomb) is the first such bomb to work by nuclear fusion and is considerably more powerful than the atomic bomb exploded over Hiroshima on August 6, 1945.
- 1952 First use of isotopes in medicine.
- 1952 The Treasury Department's Bureau of Internal Revenue (BIR) becomes the Internal Revenue Service (IRS). BIR's Alcohol Tax Unit—latest in a series of offices through which Treasury has enforced federal alcohol, tobacco, and firearms policy over the years—becomes the IRS Alcohol and Tobacco Tax Division.
- 1952 Greece and Turkey join NATO.
- 1952 First U.S. overflights of Soviet airspace, using B-47 Stratojets.
- 1952 In National Security Council Intelligence Directive (NSCID) No. 9, a secret memorandum issued on October 24, President Truman establishes the U.S. National Security Agency (NSA).
- 1952 McCarran-Walter Act is revised. The new immigration quota laws allow more Asians but exclude "subversives" and give the attorney general the right to deport immigrants found to be communists even after they acquired U.S. citizenship.
- 1952 Great Britain explodes its first nuclear device.
- 1953 Joseph Stalin dies and a political power struggle starts in the U.S.S.R.
- 1953 James D. Watson and Francis H. C. Crick publish two landmark papers in the journal *Nature*. The papers are titled "Molecular Structure of Nucleic Acids: A Structure for Deoxyribose Nucleic Acid" and "Genetic Implications of the Structure of Deoxyribonucleic Acid." Watson and Crick propose a double helical model for DNA and call attention to the genetic implications of their model. Their model is based, in part, on the x-ray crystallographic work of Rosalind Franklin and the biochemical work of Erwin Chargaff. Their model explains how the genetic material is transmitted.
- 1953 U.S. Federal Security Agency becomes the Department of Health, Education, and Welfare (HEW).
- 1953 United States receives information on VX nerve agent production from United Kingdom and sets up lab in Edgemont, Maryland to study it.
- 1953 U.S. president Dwight D. Eisenhower delivers "Atoms for Peace" speech to the UN, calling for the creation of an organization to control and develop the use of atomic energy. He later publicly predicts the potential for a nuclear arms race between the United States and the Soviet Union.
- 1953 An armistice on July 27 brings an end to the Korean War.

- 1953 In August, Operation AJAX, conducted by British and American intelligence, deposes Iraqi prime minister Mohammad Mossadegh, and restores Shah Mohammad Reza Pahlavi to the throne.
- 1954 CIA-supported coup in Guatemala overthrows President Jacobo Arbenz.
- 1954 U.S. policy of massive retaliation to any Communist aggression (forerunner of MAD—Mutually Assured Destruction—policy).
- 1954 French garrison at Dien Bien Phu falls to Viet Minh on May 7, and in July, French agree to leave Vietnam.
- 1954 Site-R, an underground government communications and operations facility in Pennsylvania, is completed.
- 1954 U.S. Navy commissions its first nuclear sub, *Nautilus*, on September 30.
- 1954 Televised Army-McCarthy hearings. Senator McCarthy focuses his hunt for communists on the highest echelons of the military, is finally denounced for his unscrupulous tactics, and is ultimately censured by the Senate.
- 1954 Manhattan Project physicist Robert Oppenheimer is stripped of his security clearance and is dismissed from government service, suspected of being a communist sympathizer.
- 1954 Atomic Energy Act is passed.
- 1954 Communist Control Act is passed, briefly outlawing the Communist Party in the United States.
- 1955 West Germany joins NATO. The Soviet Union and eight Eastern European states respond by forming the Warsaw Pact.
- 1955 National Institutes of Health organizes a Division of Biologics Control within FDA, following a death caused by a faulty polio vaccine.
- 1955 Cesium atomic clock developed.
- 1955 Boeing B-52 Stratofortress introduced.
- 1955 U.S. Navy Fleet Intelligence Center Pacific (FICPAC) established.
- 1955 ASA expands its mission to include electronic intelligence and electronic warfare functions that had formerly been the responsibility of the signal corps. Because its role now encompasses more than intelligence and security, it is reassigned from G-2 (military intelligence) to the U.S. Army Chief of Staff.
- 1955 The Berlin tunnel (operational from March 1955 until its discovery by Soviet troops in April 1956) allowed Western intelligence agencies to tap Soviet and East German communications.
- 1955 President Eisenhower signs a bill authorizing \$46 million for construction of a CIA Headquarters Building.
- 1955 A United Airlines DC-6B explodes near Longmont, Colorado, on October 1, killing all 39 passengers and 5 crewmembers. The FBI provides assistance from its Disaster Squad in identifying the deceased.
- 1955 In December, U.S. Air Force launches Project GENETRIX, a surveillance operation using balloons over communist countries. The unsuccessful effort comes to an end three months later.
- 1955 President Eisenhower sends first U.S. military and civilian advisers into Vietnam, which in 1955 is divided into northern and southern portions.
- 1956 President Eisenhower establishes the President's Board of Consultants on Foreign Intelligence Activities, predecessor to the President's Foreign Intelligence Advisory Board.
- 1956 First U-2 overflight of Soviet Union on July 5.
- 1956 Hungarian revolution is crushed by Soviet military.
- 1956 Suez Crisis when Western powers, worried over Egyptian president Gamal Abdel Nasser's close ties with the Soviet bloc, refuse assistance in building Aswan High Dam. In response, Nasser seizes the Suez Canal. Britain and France form an alliance with Israel, which invades on October 26.
- 1956 Fidel Castro launches Cuban revolution against the Batista regime.
- 1956 Soviet First Secretary Nikita Khrushchev, speaking about the West, states "History is on our side. We will bury you." The following year, he becomes premier of the Soviet Union.
- 1956 Pakistan officially becomes an Islamic state.
- 1957 International Atomic Energy Agency (IAEA) is formed as an autonomous UN body to verify that nuclear materials are not used in a prohibited manner.
- 1957 In March, President Eisenhower proclaims the Eisenhower Doctrine, whereby "the United States regards as vital to the national interest and world peace the preservation of the independence and integrity of the nations of the Middle East."
- 1957 The Soviet Union launches *Sputnik*.
- 1957 Civil Rights Act of 1957 establishes U.S. Commission on Civil Rights.
- 1957 The sodium reactor experiment at Santa Susana, California, provides the first power generated from a civilian nuclear reactor.
- 1957 June 21, the FBI arrests Colonel Rudolf Ivanovich Abel, a Soviet espionage agent.
- 1957 United States conducts first underground nuclear test in a tunnel 100 miles from Las Vegas.
- 1958 U.S. National Defense Education Act dedicates resources to math, science, and language education.
- 1958 United States establishes NASA (the National Aeronautics and Space Administration).
- 1958 Explorer 1, the first U.S. satellite, launched with a cosmic ray detector onboard.
- 1958 U.S. Department of Defense establishes Advanced Research Projects Agency (ARPA).
- 1958 The Federal Aviation Act passes, creating the Federal Aviation Agency.
- 1958 Congress passes Defense Reorganization Act, which creates unified military commands within the U.S. Department of Defense.

- 1958 United States conducts nuclear tests high above the Pacific Ocean. The explosions send out an extremely high-frequency electromagnetic pulse that turns off street lights in Hawaii and disrupts radio navigation as far away as Australia for up to 18 hours.
- 1958 Iraqi monarchy is overthrown in a military coup.
- 1958 Following the Geneva Conference on the Discontinuance of Nuclear Weapons Tests, the United States, Great Britain, and Soviet Union declare temporary testing moratoriums.
- 1959 The microchip, forerunner of the microprocessor, is invented.
- 1959 Fidel Castro takes power in Cuba on January 1.
- 1959 Launch of the *Forrestal*, the first of many large carriers deployed by the U.S. Navy. The *Forrestal* includes rectangular extensions on the rear part of the flight deck, which greatly expand the deck area.
- 1959 U.S. Navy's Marine Mammal Program established near Los Angeles, CA.
- 1959 Discoverer XIV, the first successful mission of the Corona satellite program, which was developed the previous year to photograph sites in the Soviet Union. The returning capsule, containing 20 pounds of film and suspended from a parachute, is snatched from midair by a U.S. C-119 aircraft.
- 1959 President Eisenhower approves a secret program, proposed by the CIA, to depose communist Cuban leader Fidel Castro.
- 1960 Chinese criticisms of the Soviet Union cause a split in Sino-Soviet relations.
- 1960 Vietcong seek to overthrow South Vietnamese president Ngo Dinh Diem.
- 1960 First U.S. KeyHole intelligence satellite launched.
- 1960 Theodore Harold Maiman, American physicist, develops the first laser. He uses a ruby cylinder that emits a light that is coherent (all in a single direction) and monochromatic (a single wavelength). He finds that it can travel thousands of miles as a beam without dispersing, and that it can be concentrated into a small, super-hot spot. Laser is an acronym for Light Amplification by Stimulated Emission of Radiation.
- 1960 France explodes its first nuclear device.
- 1960 Premier Nikita Khrushchev vows the Soviet Union will support "wars of national liberation."
- 1960 The NSA begins intercepting messages and communications revealing the Soviet military buildup in Cuba, including the installation of air defense systems and missile capabilities.
- 1960 U.S. Navy Fleet Intelligence Center Europe (FICEUR) established.
- 1960 Defense Information Systems Agency (DISA) established as Defense Communications Agency.
- 1960 In September, NSA cryptographers William H. Martin and Bernon F. Mitchell defect to the Soviet Union and issue the first public revelations as to NSA's mission.
- 1960 A Soviet missile shoots down an American U-2 spy plane near Sverdlovsk. The pilot Francis Gary Powers is detained and tried by the Soviet Union as a spy. After nearly two years, Powers is exchanged for a captured Soviet spy. Soviet outrage over the incident leads to the collapse of the Paris summit of the Conference on Discontinuance of Nuclear Weapons Trials.
- 1961 In his inauguration speech, President John F. Kennedy sets the tone for modern U.S. foreign policy when he states, "Let every nation know, whether it wishes us well or ill, that we shall pay any price, bear any burden, meet any hardship, support any friend, oppose any foe to assure the survival and success of liberty."
- 1961 National Photographic Interpretation Center (NPIC) formed.
- 1961 U.S. Strategic Air Command activates its Airborne Command Post on February 3. Known as Looking Glass for the fact that equipment aboard its planes mirrors control systems on the ground, Looking Glass will remain in continuous operation for the next 29 years.
- 1961 Soviet Union launches first cosmonaut, Yuri Gagarin, into space.
- 1961 Cuba establishes what will become its largest intelligence agency, the Dirección General de Inteligencia (DGI; General Intelligence Directorate), within the Ministry of the Interior.
- 1961 Cuban exiles organized and armed by the CIA invade Cuba on April 17, in a failed attempt to overthrow the leftist leader Fidel Castro. The event became known as the "Bay of Pigs," in reference to the small bay on the southern coast of Cuba where the invasion commenced.
- 1961 Congress creates the U.S. Arms Control and Disarmament Agency (ACDA), devoted to policy making for conventional and nuclear armament.
- 1961 United States introduces the first nuclear-powered aircraft carrier, the *Enterprise*.
- 1961 First U.S. aircraft hijacking on May 1. The hijacker takes over the plane at gunpoint and forces pilots to fly to Havana, Cuba, where he is granted asylum.
- 1961 In August, the Soviet Union and East Germany erect the Berlin Wall to divide West and East Berlin.
- 1961 In a letter published in the September issue of *Life* magazine, President Kennedy advises Americans to build fallout shelters to reduce American vulnerability to Soviet nuclear attack. "Shelter-mania" ensues as Americans prepare for potential nuclear attack.
- 1961 Defense Intelligence Agency established.
- 1961 Soviet Union resumes nuclear weapons testing after dispute on verification provisions of test ban agreements. Two weeks later the United States resumes testing.
- 1962 Commissioning of the first Navy SEAL (sea, air, land) teams.

- 1962 Cuban missile crisis, triggered by the Soviet deployment to Cuba of medium-range, nuclear-armed ballistic missiles, brings the world to the brink of nuclear war. The United States blockades Cuba for 13 days until the Soviet Union agrees to remove its missiles. The United States also agrees to remove its missiles from Turkey. The crisis marks the first time the NSA creates an around-the-clock command center.
- 1962 During the Cuban Missile Crisis in October, President Kennedy becomes concerned with faulty communications technology in the national security communications apparatus. After the crisis ends, he calls for a study to improve communications coordination and technology, ultimately leading to the formation of the National Communication System.
- 1963 A nuclear submarine, the USS *Thresher*, sinks off the coast of Cape Cod in 8,400 feet of water, killing all 129 sailors aboard.
- 1963 Development of Canada Geographic Information System, the first modern geographic information system, begins.
- 1963 Coup in Iraq led by the Arab Socialist Ba'ath Party (ASBP).
- 1963 Directorate of Science and Technology, the arm of the CIA responsible for technological development, is formed.
- 1963 Britain's war minister, Lord John Dennis Profumo, is discovered to be sleeping with Christine Keeler, who is also having an affair with a Soviet spy. The scandal becomes known as the Profumo affair.
- 1963 Israel's Mossad assists in the defection of an Iraqi airman, who delivers to Israel a Soviet MiG-21 fighter jet.
- 1963 The United States and Soviet Union set up a hotline (teletype) between the White House and the Kremlin.
- 1963 The United States and Soviet Union sign the Limited Test Ban Treaty, which prohibits underwater, atmospheric, and outer space nuclear tests. More than 100 countries have ratified the treaty since 1963.
- 1963 Assassination of South Vietnamese President Ngo Dinh Diem on November 1.
- 1963 November 22, Lee Harvey Oswald assassinates President Kennedy in Dallas, Texas. Lyndon B. Johnson becomes president.
- 1964 American refusal to fly the Panamanian flag over a high school in the Panama Canal Zone sparks riots that leave 23 Panamanians and four U.S. Marines dead. Afterward, Panama calls for new treaty discussions with the United States.
- 1964 U.S. Navy introduces E-2 Hawkeye airborne early warning and command and control aircraft.
- 1964 North Vietnamese gunboats open fire on U.S. destroyer *Maddox* in the Gulf of Tonkin on August 2. This results in the Gulf of Tonkin resolution, passed by U.S. Senate, which gives President Johnson power to vastly escalate U.S. commitment in Vietnam.
- 1964 China conducts its first nuclear test.
- 1965 American troops sent to the Dominican Republic to prevent a communist takeover.
- 1965 Congress passes Drug Abuse Control Amendments—legislation that forms the FDA Bureau of Drug Abuse Control and gives the FDA tighter regulatory control over amphetamines, barbiturates, and other prescription drugs with high abuse potential.
- 1965 Congress authorizes protection of former presidents and their spouses during their lifetime and minor children until age 16.
- 1965 In June, first U.S. ground troops arrive in Vietnam.
- 1965 Anthrax vaccine adsorbed (AVA), is approved for use in the United States.
- 1965 First bombings against Israel by the Palestine Liberation Organization (PLO).
- 1966 France withdraws its troops from the North Atlantic Treaty Organization (NATO). French President de Gaulle argues for a Europe free from both American and Soviet intervention.
- 1966 Marshall Nirenberg and Har Gobind Khorana lead teams that decipher the genetic code. All of the 64 possible triplet combinations of the four bases (the codons) and their associated amino acids are determined and described.
- 1966 NORAD Combat Operations Center in Cheyenne Mountain becomes fully operational.
- 1966 Naval Investigative Service, predecessor of the Naval Criminal Investigative Service, formed as an office within the Office of Naval Intelligence.
- 1967 FBI's National Crime Information Center (NCIC) becomes operational.
- 1967 Congress passes Freedom of Information Act, which limits the ability of U.S. federal government agencies to withhold information from the public by classifying that information as secret.
- 1967 In the Six-Day War, fought in the first week of June, Israel defeats a much larger Arab force, and gains control of the west bank of the Jordan River, which was previously Jordanian territory.
- 1967 CIA launches Phoenix program to fight Vietcong infrastructure in South Vietnam.
- 1967 A cosmic gamma ray burst leads to the discovery of a new phenomenon for astronomers to study. The burst is detected while U.S. Vela spy satellites remain alert for potential Soviet nuclear testing in space. Part of an unclassified research and development program, the Vela program was designed to develop nuclear monitoring technology. Vela satellites carried x-ray, gamma-ray, neutron detectors, EMP detectors and other instruments.
- 1968 An overwhelming North Vietnamese attack on South Vietnamese cities, called the Tet Offensive, ultimately proves to be a crucial psychological turning point in the Vietnam War.
- 1968 FDA administratively moves to Public Health Service.



- 1968 During testing exercise of VX nerve agent, 6,400 sheep are killed near Dugway, Utah.
- 1968 Following passage of the Gun Control Act, the Alcohol and Tobacco Tax Division of IRS becomes the Alcohol, Tobacco, and Firearms (ATF) Division.
- 1968 U.S. Navy Fleet Intelligence Center Atlantic (FICLANT) established.
- 1968 U.S. anti-drug agencies in the Treasury and Health, Education, and Welfare departments merged to form the Bureau of Narcotics and Dangerous Drugs under the Justice Department.
- 1968 National Institute of Justice established under the authority of the Omnibus Crime Control and Safe Streets Act to provide independent, evidence-based tools to assist state and local law enforcement.
- 1968 Creation of first national contingency plan to deal with oil spills in the United States.
- 1968 Israel's Mossad successfully captures eight missile boats that Israel had ordered from France, but which President Charles de Gaulle had placed under embargo. Mossad also captures and brings to trial nuclear technician Mordechai Vanunu, who had revealed Israeli nuclear secrets to the British press.
- 1968 Prague Spring reforms in Czechoslovakia ended by Soviet invasion.
- 1968 James Earl Ray assassinates Dr. Martin Luther King Jr. in Memphis, Tennessee, on April 4. The FBI opens a special investigation based on the violation of Dr. King's civil rights so that federal jurisdiction in the matter can be established.
- 1968 As a result of Senator Robert F. Kennedy's assassination on June 5, Congress authorizes protection of major presidential and vice-presidential candidates and nominees.
- 1968 Nuclear Nonproliferation Treaty (NPT)—calling for halting the spread of nuclear weapons capabilities—is signed.
- 1968 Final flight of X-15 hypersonic aircraft on October 24.
- 1969 President Richard Nixon begins troop withdrawal from Vietnam.
- 1969 On July 20, U.S. astronaut Neil Armstrong becomes the first man to walk on the moon.
- 1969 Strategic Arms Limitation Talks (SALT) begin between the United States and the Soviet Union.
- 1969 United States and Soviet Union begin period of diplomatic détente.
- 1969 By Executive Order, the United States renounces first-use of biological weapons and restricts future weapons research programs to issues concerning defensive responses (e.g., immunization, detection, etc.).
- 1969 Microprocessor developed.
- 1969 Defense Department's Advanced Research Projects Agency (ARPA) establishes ARPANET, a forerunner to the Internet.
- 1969 Muammar Qaddafi seizes power from King Idris in Libya on September 1.
- 1970 The National Environmental Policy Act of 1969 is signed, requiring the federal government to review the environmental impact of any action—such as construction of a building—that might significantly affect the environment.
- 1970 United States Congress passes Controlled Substance Act (CSA), delineating a hierarchy of commonly abused drugs and establishing corresponding penalties for misuse.
- 1970 United States Environmental Protection Agency established.
- 1970 White House Police Force renamed the Executive Protective Service.
- 1970 The UN assigns the International Atomic Energy Agency (IAEA) the task of NPT monitoring and for developing nuclear safeguards.
- 1970 The Consolidated Federal Law Enforcement Training Center, a bureau of the Department of the Treasury, is established as an organization to provide training for all federal law-enforcement personnel. Today known as the Federal Law Enforcement Training Center, it is now part of the Department for Homeland Security.
- 1970 In October, a group advocating the separation of Quebec from Canada kidnaps two government officials and murders one of them. The crisis causes the temporary imposition of martial law in the country and renews calls for a dedicated security agency.
- 1970 Congress approves the Organized Crime Control Act in October. This law contains a section known as the Racketeer Influenced and Corrupt Organization Act or RICO. RICO becomes an effective tool in convicting members of organized criminal enterprises.
- 1971 CIA activity in Laos, termed by critics a "secret war," is exposed.
- 1971 Chinese defense minister Lin Biao attempts a coup against Mao Zedong but is killed in a plane crash. China is officially seated in the UN and launches its first space satellite.
- 1971 Stolen by Defense Department official Daniel Ellsberg, a classified set of papers detailing compromising U.S. involvement in Vietnam, "The Pentagon Papers," is published by the *New York Times* and the *Washington Post*.
- 1971 United Kingdom passes the Misuse of Drugs Act.
- 1971 Canada Geographic Information System becomes operational.
- 1971 Congress authorizes Secret Service protection for visiting heads of a foreign state or government, or other official guests, as directed.
- 1971 The NSA receives operation control over the cryptologic agencies of the air force, army and navy. The three agencies are reorganized into the newly created Central Security Service (CSS) headed by the NSA director. The move centralizes the government's

- signals intelligence (SIGINT) and communications security (COMSEC) programs under the NSA.
- 1971 Spy satellite called *Hexagon* is launched carrying a KH-9 camera.
- 1972 U.S. president Nixon meets with Mao Zedong in Beijing. The meeting eases U.S.-China animosities.
- 1972 President Nixon visits Soviet Union.
- 1972 United States and Soviet Union under Premier Leonid Brezhnev negotiate reductions in nuclear arsenals.
- 1972 Defense Investigative Service (changed in 1997 to Defense Security Service) established on January 1.
- 1972 Recombinant technology emerges as one of the most powerful techniques of molecular biology. Scientists are able to splice together pieces of DNA to form recombinant genes. As the potential uses, therapeutic and industrial, become increasingly clear, scientists and venture capitalists establish biotechnology companies.
- 1972 *Landsat 1* satellite launched, providing the first publicly available satellite imagery.
- 1972 Congress passes the Consumer Product Safety Act, creating the Consumer Product Safety Commission, which is charged with protecting the public from risk or injury involved with defective or unsafe products.
- 1972 The ATF Division of IRS becomes a separate Treasury bureau, the Bureau of Alcohol, Tobacco, and Firearms.
- 1972 Computer axial tomography, commonly known as CAT scanning, is introduced. A CAT scan combines many high-definition, cross-sectional x-rays to produce a two-dimensional image of a patient's anatomy.
- 1972 President Nixon issues Executive Order 11652, which stipulates that virtually all national security records should be declassified after 30 years.
- 1972 Five men ultimately discovered to have ties to anti-Castro forces, the American CIA, and the White House are arrested inside the Democratic National Headquarters at the Watergate Hotel in Washington, D.C. Known as a "plumbers" team, the intelligence operatives carried electronic surveillance equipment and cameras. A subsequent cover-up of the break-in, destruction of taped conversations related to the cover-up, and revelations of a history political dirty tricks form the core of the Watergate scandal that ultimately leads to criminal prosecutions of top officials and President Nixon's resignation in August 1974.
- 1972 The Antiballistic Missile (ABM) Treaty is signed by the United States and the Soviet Union. The treaty is one of two treaties produced by the first series of Strategic Arms Limitation Talks (SALT I) between the two countries; the other is an interim agreement limiting offensive nuclear weapons.
- 1972 U.S. Department of Defense directs Advanced Research Projects Agency (ARPA) name change to the Defense Advanced Research Projects Agency (DARPA) in March. DARPA is established as a separate defense agency under the Office of the Secretary of Defense.
- 1972 The FBI Academy opens a new training facility on the Marine Corps Base at Quantico, Virginia in May.
- 1972 Biological and Toxin Weapons Convention first signed. BWC prohibits the offensive weaponization of biological agents (e.g., anthrax spores). The BWC also prohibits the transformation of biological agents with established legitimate and sanctioned purposes into agents of a nature and quality that could be used to effectively induce illness or death.
- 1972 "Bloody Friday": on July 21, an IRA bomb attack kills 11 people and injures 130 in Belfast, Northern Ireland. Ten days later, three additional IRA attacks in the village of Claudy leave six dead.
- 1972 Establishment of U.S. Air Force Intelligence Service in June.
- 1972 After 11 Israeli athletes are murdered by Palestinian terrorists with the Black September organization at the Munich Olympics in September, Israel's Mossad establishes an action team, Wrath of God. Over the next two years, the team tracks down and kills a dozen members of Black September.
- 1972 Iraq and Soviet Union sign 15-year Treaty of Friendship and Cooperation.
- 1973 The peace treaty ending the Vietnam War, the Paris Peace Accords, is signed. South Vietnam collapses two years later after the last U.S. troops are withdrawn.
- 1973 Atmospheric Release Advisory Capability (ARAC) concept has its origins when the Department of Energy (DOE) seeks assistance from scientists at California's Lawrence Livermore National Laboratory in assessing potential and ongoing atmospheric hazards.
- 1973 Concerns about the possible hazards posed by recombinant DNA technologies, especially work with tumor viruses, leads to the establishment of a meeting at Asilomar, California. The proceedings of this meeting are subsequently published by the Cold Spring Harbor Laboratory as a book entitled *Biohazards in Biological Research*.
- 1973 Drug Enforcement Administration (DEA) created on July 1.
- 1973 Libya claims the Gulf of Sidra in defiance of international protocol.
- 1973 General Augusto Pinochet, with the support of the CIA, overthrows Marxist president Salvador Allende in Chile in September. Allende dies—either by suicide (according to Pinochet) or by murder (according to Allende's supporters).
- 1973 Arab-Israeli Yom Kippur War. Fourth Arab-Israeli war begins with a combined Egyptian and Syrian attack against Israel in October. When military efforts fail, the Organization of Petroleum-Exporting Countries (OPEC) announces a cutback in oil production, raising gasoline prices and precipitating an energy crisis in the United States.

- 1974 Congress passes the Energy Reorganization Act, which abolishes the Atomic Energy Commission (AEC) and replaces it with two other agencies: the Nuclear Regulatory Commission (NRC) and the Energy Research and Development Administration.
- 1974 Members of the Symbionese Liberation Army (SLA) kidnap heiress Patricia Hearst on February 5. Hearst, allegedly brainwashed by the group, adopts the name "Tania" and participates in bank robberies. Most members, including leader Donald DeFreeze, are killed in a May 1974 shootout with authorities, and Hearst is captured by the FBI in September 1975. In January 2001, outgoing president William J. Clinton pardons her.
- 1974 Treaty on Underground Nuclear Weapons Tests (also known as the Threshold Test Ban Treaty) is signed by the United States and Soviet Union, prohibiting underground nuclear weapons tests using weapons that produce yields greater than 150 kilotons.
- 1974 U.S. Navy Fleet Intelligence Center (FIC) Europe (FICEUR) and FIC Atlantic (FICLANT) merge to form FIC Europe-Atlantic (FICEURLANT).
- 1974 Cuba's National Liberation Directorate (DLN), which is responsible for fomenting communist revolutions worldwide, becomes the America Department (DA) of the Communist Party of Cuba Central Committee. During the years that follow, DA will provide support to communist insurgents and terrorists in numerous locales.
- 1974 Congress passes Privacy Act of 1974, greatly restricting the authority of agencies to collect information on individuals, or to disclose that information to persons other than the individual. The Privacy Act also requires agencies to furnish individuals with any information on them that the agency has in its files.
- 1974 New era of congressional oversight in intelligence begins with passage of Hughes-Ryan Act amending the Foreign Service Act. Written in the wake of covert activities that helped bring down the Marxist regime of Salvador Allende in Chile, Hughes-Ryan requires the president to submit plans for covert actions to the relevant congressional committees.
- 1974 The *New York Times* publishes a report concerning a CIA domestic intelligence campaign involving interception of private mail.
- 1974 India conducts its first nuclear test—an explosion in the Rajasthan Desert.
- 1974 British Prevention of Terrorism Act permits the arrest of suspected terrorists without a warrant and allows authorities to detain them for a week without bringing charges. While being interned, detainees are subject to a range of harsh practices that include "hooding"—being isolated and forced to wear a hood over their heads—noise bombardment, and sleep and food deprivation.
- 1974 Bar-coded products arrive in American stores, along with the laser scanners used at checkout stations to read the codes.
- 1975 American Apollo 18 and Soviet Soyuz 19 join in an orbital linkup.
- 1975 Puerto Rican nationalists bomb a Wall Street bar, killing four and injuring 60; two days later, the Weather Underground claims responsibility for an explosion in a bathroom at the U.S. Department of State in Washington.
- 1975 The duties of Executive Protective Service are expanded to include protection of foreign diplomatic missions located throughout the United States and its territories.
- 1975 U.S. Nuclear Emergency Support Team established to analyze and respond to cases involving nuclear threats.
- 1975 On April 30, Saigon falls to North Vietnamese. In the following year, Vietnam is united under a communist government.
- 1975 Commissioning, in May, of the *Nimitz*, first in a super-class of large modern aircraft carriers deployed by the U.S. navy.
- 1975 President Gerald R. Ford signs Executive Order 11828, creating the Commission on CIA Activities within the United States.
- 1975 Investigations by congressional committees headed by Idaho senator Frank Church and New York representative Otis Pike reveal that government agencies, including the NSA, performed clandestine surveillance on U.S. citizens who participated in the civil rights and anti-Vietnam War movements.
- 1975 FBI special agents Jack R. Coler and Ronald A. Williams are murdered while conducting an investigation on an Indian reservation in South Dakota. American Indian Movement leader Leonard Peltier is convicted of committing the murders.
- 1975 President Ford escapes an assassination attempt in Sacramento, California, by Lynette Alice (Squeaky) Fromme, who pointed a gun at him but did not fire. A few weeks later, Ford escaped another assassination attempt in San Francisco, California, when Sara Jane Moore was prevented from firing at him by a bystander.
- 1976 Chinese Premier Zhou Enlai and Central Committee Chairman Mao Zedong die.
- 1976 Church Committee submits its final report on April 26. Meanwhile, on January 29, just two days before the Pike Committee was to complete its investigation, the House votes not to make its findings public. (The report was later leaked to journalist Daniel Schorr, who passed it on to the *Village Voice*.)
- 1976 On May 19, the Senate establishes its permanent Select Committee on Intelligence. On July 14, 1977, the House puts in place its own such committee.
- 1976 On the night of July 3–4, members of Israel's Mossad conduct a raid on a French airliner, hijacked by Palestinian terrorists, in the Ugandan city of Entebbe. The Israelis rescue all but four of the plane's 97 passengers, losing a single officer, along with 20 Ugandan soldiers, in the process.
- 1976 A military junta overthrows the government of Argentina.

- 1977 The United States vetoes a UN Security Council resolution calling for total Israeli withdrawal from Arab areas.
- 1977 U.S. ambassador Francis E. Melroy is killed in Beirut.
- 1977 U.S. president James E. Carter and Panamanian military dictator Omar Torrijos sign the Panama Canal Treaty on September 7, which abolishes the Canal Zone, terminates all prior treaties regarding the canal, and provides for the full transfer of the canal to Panama on December 31, 1999. A separate Neutrality Treaty guarantees the neutrality of the canal in perpetuity. Congress ratifies both treaties the following year.
- 1977 Introduction of E-3 Sentry AWACS (airborne warning and control system). Packed with electronics, the aircraft—based on the Boeing 707—serves purposes that include identifying enemy aircraft, jamming enemy radar, guiding bombers to their targets, and managing the flow of friendly aircraft.
- 1977 The last reported smallpox case recorded. Ultimately, the WHO declares the disease eradicated.
- 1977 Office of Intelligence Support (OIS) established as the intelligence office of the U.S. Department of the Treasury. OIS thus replaces Office of National Security, established in 1961.
- 1977 U.S. Army Intelligence and Security Command (INSCOM) goes into operation on January 1.
- 1977 In November, Delta Force is activated. Established by Colonel Charles Beckwith at Fort Bragg, North Carolina, Delta Force becomes one of the leading U.S. counterterrorist units.
- 1977 A new security and intelligence command known as Headquarters, U.S. Army Intelligence and Security Command, replaces ASA.
- 1977 Department of Energy Organization Act signed into law by President Carter on October 1. The U.S. Department of Energy (DOE) replaces the Energy Research and Development Administration and consolidates Federal energy programs and activities.
- 1978 The United States recognizes the People's Republic of China (PRC).
- 1978 On January 24, President Carter signs Executive Order 12036, "United States Foreign Intelligence Activities," which restructures the U.S. Intelligence Community and provides explicit guidance on all facets of intelligence activities.
- 1978 A bomb disguised as a package goes off at Northwestern University. This is the first of 16 attacks, over the course of 17 years, by an individual dubbed the "Unabomber" for his principal targets, universities and airlines.
- 1978 Camp David meetings between U.S. president Carter, Egyptian president Anwar Sadat, and Israeli prime minister Menachem Begin, offer hope for peace in Middle East.
- 1978 Dissident Georgi Markov is assassinated by an umbrella tip laced with ricin in London by the Bulgarian secret service.
- 1978 Congress passes the Foreign Intelligence Surveillance Act to regulate electronic intelligence gathering. The act includes the creation of a special court to handle requests by the NSA to perform electronic surveillance on targeted U.S. persons.
- 1978 Executive Order 12046 establishes National Telecommunications Information Administration to serve as president's advisory on matters involving the radio frequency spectrum.
- 1978 President Carter, in Executive Order 12065, calls for a review of national security records after 20 years with an eye toward declassification.
- 1978 DOE initiates its Nuclear Threat Assessment Program at Lawrence Livermore National Laboratory in September.
- 1978 The U.S. government defines a cipher algorithm for standard use by all government departments, the Digital Encryption Standard.
- 1978 Kidnapping of Italian former prime minister Aldo Moro; he was seized by the Red Brigade and assassinated 55 days later.
- 1978 The United States cancels development of the neutron bomb, which would theoretically destroy life but cause minimal physical destruction. The bomb was initially developed, in part, to ensure the maximal survival of European cultural treasures in the advent of nuclear war and thus enhance the credibility of U.S. threats to use the bomb against possible Soviet aggression in western Europe.
- 1978 The FBI Laboratory Division begins use of laser technology to detect latent crime scene fingerprints.
- 1979 Egyptian president Sadat and Israeli prime minister Begin sign a peace treaty; other Arab nations protest the treaty.
- 1979 Congress passes Panama Canal Act. Among its many provisions, the act creates the Panama Canal Commission, which will act as custodian over the canal for the next 20 years.
- 1979 Sandinistas gain control of Nicaragua.
- 1979 As a result of a March 28 accident at the Three Mile Island plant outside Harrisburg, Pennsylvania, portions of the reactor's core melts, potentially threatening the health and perhaps even the lives of nearby residents. For several weeks, the nation is gripped by terror as government agencies, including the Nuclear Regulatory Commission, respond to the disaster. No deaths occur as a result of the Three Mile Island accident, but construction of new commercial reactors will be delayed for more than two decades. ARAC and the National Atmospheric Release Advisory Center (NARAC) at Livermore first prove their capabilities by providing DOE and other federal agencies with assessment of the incident.
- 1979 Use of illegal drugs in the United States reaches its peak, as three out of 10 youth, and one in five adults, reports having used an illegal substance.
- 1979 President Carter issues an executive order creating the Federal Emergency Management Agency (FEMA).

- 1979 Saddam Hussein becomes president of Iraq.
- 1979 The Iranian shah flees Iran, and Shiite Muslim leader Ayatollah Khomeini assumes control of the fundamentalist Islamist revolution. The shah, suffering from cancer, seeks treatment and asylum in the United States. Islamist revolutionaries (mostly Iranian students) seize the American embassy and take 66 Americans hostage. Thirteen hostages are soon released, but the remaining 53 are held until January 20, 1981. The hostage crisis consumes the remainder of U.S. president Carter's term and critics claim that his failure to act decisively to secure the release of the hostages ultimately emboldens a generation of Islamist fundamentalists to commit acts of terrorism against the United States.
- 1979 Less than a month after the seizure of the U.S. embassy in Tehran, the U.S. embassies in Tripoli, Libya, and Islamabad, Pakistan, are attacked.
- 1979 Soviets invade Afghanistan on December 24.
- 1980 CNN, the first 24-hour-a-day cable television news channel, is launched, inspired in part by intense public interest in the Iranian hostage crisis.
- 1980 After Lech Walesa leads a strike by shipyard workers, Poland's Solidarity Party becomes an independent labor union, the first in the sphere of Soviet influence.
- 1980 More than five months after the seizure of the U.S. embassy in Tehran, Iran, the United States mounts an attempt to rescue the hostages, but fails when helicopters collide in the desert. The crash forces leaders to abort the mission. Eight Americans die and five are injured in the attempt.
- 1980 The U.S. Supreme Court rules that a living organism developed by General Electric (a microbe used to clean up an oil spill) can be patented.
- 1980 Congress passes the Classified Information Procedures Act, which presents guidelines for the use of classified information by both the government and defendants in legal cases.
- 1980 The United States and 57 other countries boycott the summer Olympics in Moscow to protest Soviet occupation of Afghanistan.
- 1980 Intelligence Oversight Act replaces the armed services committees with intelligence committees as the principal arm of legislative oversight over the CIA in both houses of Congress.
- 1980 Iran shells Iraqi border installations at the start of the Iran/Iraq war. Two weeks later, Iraq attacks Iranian air bases.
- 1980 The Comprehensive Environmental Response, Compensation, and Liability Act (also known as Superfund) is passed in response to the discovery in the late 1970s of a large number of abandoned, leaking hazardous waste dumps. Under Superfund, the Environmental Protection Agency identifies hazardous sites, takes appropriate action, and sees that the responsible party pays for the cleanup.
- 1980 The Low-Level Radioactive Waste Policy Act is passed, making states responsible for the disposal of their own low-level nuclear waste, such as from hospitals and industry.
- 1981 AIDS (Acquired Immune Deficiency Syndrome) is recognized and tracked as an epidemic.
- 1981 Ronald Reagan inaugurated as president of the United States. Fearing Reagan's promise to renew and use American military strength to protect U.S. citizens and interests, Islamist militant revolutionaries in Iran release U.S. hostages held for 444 days.
- 1981 President Ronald Reagan signs Intelligence Authorization Act of 1981, mandating congressional oversight of covert actions. As part of its oversight of the intelligence community, Congress has passed intelligence authorization acts in every fiscal year since.
- 1981 President Reagan wounded in assassination attempt by John W. Hinckley, Jr.; three others also wounded.
- 1981 Israel launches air attacks to destroy an Iraqi nuclear research center at Tuwaythah, Iraq, a city near Baghdad.
- 1981 In August, two U.S. F-14 Tomcat fighters dispatched by the U.S. Sixth Fleet shoot down two Libyan Su-22 fighter-bombers over the Gulf of Sidra.
- 1981 Egyptian president Anwar Sadat assassinated by Islamic militants on October 6.
- 1981 President Reagan reconstitutes the President's Foreign Intelligence Advisory Board and names 19 distinguished citizens outside of government to serve on the Board.
- 1981 President Reagan signs Executive Order 12333 on December 4, which clarifies ambiguities of previous orders and sets clear goals for the Intelligence Community in accordance with law and regard for the rights of Americans.
- 1981 Murder of missionaries, December 4: three American nuns and one lay missionary are found murdered outside San Salvador, El Salvador. They are assumed to have been assassinated by a right-wing death squad.
- 1981 In order to avoid mid-air collisions of increasingly traveled skies, the FAA adopts the aircraft Traffic Alert and Collision Avoidance Systems I and II (TCAS I and II). The system combines radio transmitters and receivers, directional antennas, and computer and cockpit displays to transmit signals called interrogations. Other airplanes in the area receive these signals and transmit replies. Finally, computers calculate the distance between the planes based on time between the interrogation and the reply.
- 1982 Israel invades Lebanon and ousts PLO forces. In consolidating its occupation of southern Lebanon, which it first invaded in 1978, Israel becomes the first nation to make significant use of unmanned reconnaissance drones in combat.
- 1982 American journalist James Bamford publishes *The Puzzle Palace*, an expose on the work of the U.S. National Security Agency.
- 1982 In January, federal law enforcement reorganization gives DEA and FBI concurrent jurisdiction in drug-related criminal matters.

- 1982** The FDA issues regulations for tamper-resistant packaging after seven people die in Chicago from ingesting Tylenol capsules laced with cyanide. The following year, the federal Anti-Tampering Act is passed, making it a crime to tamper with packaged consumer products.
- 1982** Spain joins NATO.
- 1982** With Executive Order 12356, President Reagan bucks the trend of earlier administrations with regard to declassification of national security materials. Reagan tightens the standards with the order, which favors continued classification and even provides conditions for the reclassification of previously declassified documents.
- 1982** United States withdraws from comprehensive test ban negotiations indefinitely.
- 1982** President Reagan signs Executive Order 12382, which establishes the National Security Telecommunications Advisory Committee (NSTAC), a presidential advisory board composed of leaders in the telecommunications, finance, and aerospace industries.
- 1982** U.S. authorities convict four Castro aides of smuggling drugs into the United States, and subsequently uncover a vast Cuban drug-smuggling ring that operates in cooperation with Panamanian leader General Manuel Noriega, as well as with Colombian drug lords.
- 1982** On June 23, President Reagan signs into law the Intelligence Identities Protection Act, making it a felony to reveal the names of covert intelligence personnel.
- 1982** In December, Congress passes Boland Amendment to War Powers Act of 1973, forbidding CIA or Department of Defense to support anti-Sandinista forces in Nicaragua.
- 1983** On January 1, U.S. Defense Department and all participants in its ARPANET officially adopt TCP/IP, a revolutionary new system for network connectivity. Some regard this event as the birth of the Internet.
- 1983** The Nuclear Waste Policy Act of 1982 is signed, authorizing the development of a high-level nuclear waste repository.
- 1983** February 13 attack on law enforcement officers in Medina, North Dakota, by the Sheriff's Posse Comitatus is the first significant incident involving an anti-government right-wing terrorist group in the United States.
- 1983** Bombing of U.S. embassy in Beirut, Lebanon, April 18: sixty-three people, including the CIA's Middle East director, are killed and 120 injured in a 400-pound suicide truck-bomb attack on the U.S. embassy. Islamic Jihad claims responsibility.
- 1983** Democratic rule is restored in Argentina.
- 1983** U.S. president Reagan terms the Soviet Union the "evil empire" and announces the Strategic Defense Initiative (Star Wars), a satellite-based defense system that can destroy incoming missiles and warheads in space.
- 1983** The FBI Hostage Rescue Team becomes fully operational.
- 1983** In October, President Reagan launches Operation Urgent Fury, the first significant U.S. military action since Vietnam, to overturn a coup on the Caribbean island of Grenada.
- 1983** Simultaneous suicide truck-bomb attacks on U.S. and French compounds in Beirut, Lebanon. A 12,000-pound bomb destroys the U.S. compound, killing 242 Americans, while 58 French troops are killed when a 400-pound device destroys a French base. Islamic Jihad claims responsibility.
- 1984** Crime-fighting efforts bolstered by the Sentencing Reform Act, which stiffens prison sentences, requiring mandatory terms for certain crimes and abolishing federal parole; and by the Victims of Crime Act. Throughout the 1980s, numerous national and community-based organizations are formed to provide support to victims of rape, spousal abuse, drunk driving, and other crimes.
- 1984** Congress enacts legislation making the fraudulent use of credit and debit cards a federal violation.
- 1984** The Canadian Security and Intelligence Service Act is approved, creating Canadian Security and Intelligence Service.
- 1984** The DOE, Office of Health and Environmental Research, U.S. Department of Energy (OHER, now Office of Biological and Environmental Research), and the International Commission for Protection Against Environmental Mutagens and Carcinogens (ICPEMC) cosponsor the Alta, Utah, conference highlighting the growing role of recombinant DNA technologies. OTA incorporates the proceedings of the meeting into a report acknowledging the value of deciphering the human genome.
- 1984** President Reagan issues a directive giving the NSA responsibility of maintaining security of government computers.
- 1984** DOE Office of Security establishes Central Training Academy. Now known as Nonproliferation and National Security Institute, this facility provides training in counterintelligence and other areas to more than 100 government departments and agencies.
- 1984** Islamic Jihad kidnaps and later murders CIA station chief William Buckley in Beirut, Lebanon. Other U.S. citizens not connected to the U.S. government are subsequently seized over a two-year period.
- 1984** With Executive Order 12472, signed on April 3, President Reagan expands the mission of the National Communications System.
- 1984** Strategic Defense Initiative Organization (SDIO) chartered in April by secretary of defense Caspar Weinberger.
- 1984** CIA Information Act, signed by President Reagan on October 15, exempts the agency from the search and review requirements of the Freedom of Information Act.
- 1984** Eighteen U.S. servicemen are killed and 83 people are injured in a bomb attack on a restaurant near a

- U.S. air force base in Spain. Hezbollah claims responsibility.
- 1984** Sikh terrorists seize the Golden Temple in Amritsar, India. One hundred people die as Indian security forces retake the Sikh holy shrine.
- 1984** Assassination of Indian prime minister Indira Gandhi, October 31; she is shot to death by members of her security force.
- 1985** Mikhail Gorbachev becomes general secretary of the Communist Party in the Soviet Union. Gorbachev institutes economic reforms and policies such as “glasnost” (openness) to ease Cold War tensions.
- 1985** Called “the year of the spy,” 1985 features a series of high-profile espionage cases and arrests. In May, the John Walker Spy Ring is arrested. Former navy personnel John Walker, Jerry Whitworth, Arthur Walker, and Michael Walker are convicted of or plead guilty to passing classified material to the Soviet Union. On November 21, Jonathan Jay Pollard, a navy intelligence analyst, is arrested for spying for Israel. On November 23, Larry Wu Tai Chin, a former CIA analyst, is arrested on charges of spying for the People’s Republic of China since 1952. On November 25, a third major spy, former National Security Agency employee William Pelton, is arrested and charged with selling military secrets to the Soviets.
- 1985** Alec Jeffreys develops “genetic fingerprinting,” a method of using DNA polymorphisms (unique sequences of DNA) to identify individuals. The method, which is subsequently used in paternity, immigration, and murder cases, is generally referred to as “DNA fingerprinting.”
- 1985** David Deutsch advances theory of quantum computing.
- 1985** Kary Mullis, working at Cetus Corporation, develops the polymerase chain reaction (PCR), a new method of amplifying DNA. This technique quickly becomes one of the most powerful tools of molecular biology. Cetus patents PCR and sells the patent to Hoffman-LaRoche, Inc. in 1991.
- 1985** The Global Positioning System (GPS) becomes operational.
- 1985** U.S. air force and army join forces to develop the J-STARS (Joint Surveillance and Target Acquisition Radar System) aircraft.
- 1985** Federal Radiological Preparedness Coordinating Committee, appointed by the Federal Emergency Management Agency (FEMA), completes the U.S. Federal Radiological Emergency Response Plan, a blueprint for the federal response to a hazard involving nuclear radiation.
- 1985** TWA hijacking, June 14: A Trans-World Airlines flight is hijacked en route to Rome from Athens by two Lebanese Hezbollah terrorists and forced to fly to Beirut. The eight crew members and 145 passengers are held for 17 days, during which one American hostage, a U.S. sailor, is murdered. After being flown twice to Algiers, the aircraft is returned to Beirut after Israel released 435 Lebanese and Palestinian prisoners.
- 1985** *Achille Lauro* hijacking, October 7: Four Palestinian Liberation Front terrorists seize an Italian cruise ship in the eastern Mediterranean Sea, taking more than 700 hostages. One elderly U.S. passenger is murdered.
- 1985** The Soviet Union announces a nuclear testing moratorium.
- 1986** The space shuttle *Challenger* explodes shortly after lift-off. Gaskets weakened by unusually cold weather are blamed for the accident, which leads to intense scrutiny of NASA safety procedures.
- 1986** Explosion at the Chernobyl nuclear plant in the Ukraine causes severe radiation leakage and an estimated 8,000 near-term deaths.
- 1986** U.S. sales of arms to Iran during its war with Iraq and the use of profits to fund anti-government, or Contra, forces in Nicaragua fuels the Iran-Contra scandal.
- 1986** DNA analysis conducted by the Scientific Intelligence Unit of England’s Scotland Yard leads to the first conviction of a criminal—Colin Pitchfork, accused of rape and murder—on the basis of DNA evidence.
- 1986** Tension escalates between the United States and Libya in the Gulf of Sidra, off the coast of Libya, as U.S. and Libyan forces skirmish. The conflict culminates on April 15 in devastating U.S. air strikes on targets within Libya.
- 1986** Congress passes Anti-Drug Abuse Act. This federal law includes mandatory minimum sentences for first time offenders with harsher penalties for possession of crack cocaine than powder cocaine.
- 1986** Computer Fraud and Abuse Act is enacted, defining federal computer crimes.
- 1986** U.S. intelligence community establishes Intelligence Community Staff Committee on MASINT (measurement and signatures intelligence) to oversee all relevant activities.
- 1986** Congress passes Emergency Planning and Community Right-to-Know Act (EPCRA), which establishes guidelines whereby federal agencies assist local communities in the event of a toxic chemical spill or related incident.
- 1986** U.S. Defense Department establishes Chemical and Biological Defense Analysis Center.
- 1986** Congress passes Goldwater-Nichols Act, the fourth major reorganization of the U.S. Department of Defense since World War II. The act calls on the White House to issue an annual National Security Strategy.
- 1986** United States Congress passes the Electronic Communication Privacy Act.
- 1986** Clayton Lonetree, the only U.S. Marine convicted of espionage, turns himself in to the CIA.
- 1987** Congress passes the Computer Security Act, which makes unclassified computing systems the responsibility of the National Institute of Standards and Technology (NIST) and not the NSA with regard to technology standards development.

- 1987 Iraqi government uses nerve agents including sarin against Kurds in Northern Iraq.
- 1987 Founding of U.S. Special Operations Command, which brings together special operations forces from the army, navy, and air force.
- 1987 The PLO's terrorist campaign against Israel becomes acute during its first Intifada (or "shaking off") of Israeli authority in the occupied territories.
- 1987 North Korean agents plant a bomb that destroys Korean Air Lines Flight 858.
- 1987 Nuclear Waste Policy Amendments Act designates Yucca Mountain, Nevada, as candidate site for the nation's first geological repository for high-level radioactive waste.
- 1987 Soviet president Gorbachev and U.S. president Reagan sign the Intermediate-Range Nuclear Forces (INF) Treaty.
- 1987 The idea to use patterns of the iris of the eye as an identification marker is patented, along with the algorithms necessary for iris identification.
- 1988 U.S. Marine Corps Lt. Col. W. Higgins is kidnapped and murdered by the Iranian-backed Hezbollah group while serving with the UN Truce Supervisory Organization (UNTSO) in Lebanon.
- 1988 Congress passes the Prescription Drug Marketing Act designed to maintain the sale and distribution of prescription drugs through legitimate commercial channels. The new law requires state-level licensing for drug wholesalers, restricts drug reimportation from other countries, institutes regulations regarding drug samples, and prohibits the traffic or counterfeiting of redeemable drug coupons.
- 1988 The Food and Drug Administration Act officially establishes the FDA as an agency of the Department of Health and Human Services. The act provides for a Commissioner of Food and Drugs appointed by the president and outlines the responsibilities of the secretary and the commissioner for research, enforcement, education, and information.
- 1988 The Human Genome Organization (HUGO) is established by scientists in order to coordinate international efforts to sequence the human genome.
- 1988 First test flight of J-STARS (Joint Surveillance and Target Acquisition Radar System) aircraft.
- 1988 Congress passes National Defense Authorization Act, establishing the Defense Nuclear Facilities Safety Board as an independent agency charged with overseeing the disposition of defensive nuclear materials.
- 1988 Iran-Iraq ceasefire begins, monitored by the UN Iran-Iraq Military Observer Group (UNIIMOG).
- 1988 The federal Polygraph Protection Act prohibits employers from using polygraphs for employment screening.
- 1988 Libyan intelligence operatives plant a bomb aboard Pan-Am flight 103, which crashes into the village of Lockerbie, Scotland, killing all 259 aboard and 11 persons on the ground. Two Libyan intelligence officers are ultimately tried under Scottish law in The Hague. One of them, Abdelbaset Ali Mohmed Al Megrahi, is found guilty in January 2001; the other, Al Amin Khalifa Fhimah, is acquitted.
- 1989 After nine years of war, Soviet forces withdraw from Afghanistan.
- 1989 British Parliament passes Security Service Act, which for the first time confers legal status on MI5.
- 1989 Charles H. Bennett and Gilles Brassard develop first quantum computer.
- 1989 United States signs Berne Convention for the Protection of Literary and Artistic Works.
- 1989 The New People's Army (NPA) assassinates U.S. army colonel James Rowe in Manila in April. The NPA also assassinates two U.S. government defense contractors in September.
- 1989 The Berlin Wall is torn down, as many communist governments in Eastern Europe collapse.
- 1989 In December, U.S. forces attack Panama to remove General Manuel Noriega in Operation Just Cause. The U.S. army uses loud music as part of a psychological operation to dislodge Noriega from his refuge at the Vatican embassy.
- 1989 Nicolae Ceausescu, communist dictator of Romania, is overthrown and executed.
- 1990 Yugoslavia overthrows Communist Party and ethnic tensions mount.
- 1990 U.S. embassy in Peru bombed by the Tupac Amaru Revolutionary Movement.
- 1990 Syrian troops intervene in Lebanon's civil war.
- 1990 Iraq invades Kuwait. UN Security Council passes resolution 660 calling for full Iraqi withdrawal. President George H.W. Bush vows "this aggression will not stand" and launches Operation Desert Shield, a buildup of U.S. forces in the region in preparation for a possible armed confrontation.
- 1990 U.S. military personnel receive vaccinations against anthrax prior to duty in the Persian Gulf.
- 1990 UN, via resolution 661, imposes economic sanctions on Iraq.
- 1990 East and West Germany reunited.
- 1990 Former Solidarity union leader Lech Walesa becomes president of post-communist Poland.
- 1990 NATO and Warsaw Pact nations sign Conventional Armed Forces in Europe treaty (CFE), which promises mutual non-aggression.
- 1990 U.S. Strategic Air Command brings to an end the 24-hour-a-day operation of its Airborne Command Post, Looking Glass, on July 24.
- 1990 Iraq hangs Farzad Bazoft, an Iranian-born journalist with the *London Observer* newspaper, whom Hussein accuses of spying on Iraqi military installations.
- 1990 Space shuttle *Atlantis* completes secret mission to place a spy satellite in orbit.



- 1991 First-ever use of the strategic petroleum reserve to stabilize world oil prices following the Iraqi invasion of Kuwait.
- 1991 Launch of Operation Desert Storm against Iraq on January 17. The initial bombing campaign lasts approximately 100 hours, and the entire military operation takes only 42 days. The result is overwhelming Iraqi defeat.
- 1991 Carbon-graphite coils capable of generating an electromagnetic pulse or otherwise disabling electronics are used in U.S.-led raids on Baghdad, Iraq.
- 1991 J-STARS aircraft gain their first combat experience in Operation Desert Storm.
- 1991 Saddam Hussein orders Iraqi forces to brutally suppress Kurd and Shia rebellions in northern and southern Iraq.
- 1991 IAEA's Iraq Action Team begins inspecting suspect sites in Iraq under UN Security Council mandate. UN also establishes a safe-haven in northern Iraq, north of latitude 36 degrees north, for the protection of the Kurds. Subsequently, the United States orders Iraq to end all military activity and establishes north and south "no-fly" zones.
- 1991 Soviet president Mikhail Gorbachev announces that the Soviet Union will unilaterally cease nuclear testing for one year.
- 1991 The United States and Soviet Union sign historic agreement to cut back long-range nuclear weapons by more than 30 percent over the next seven years.
- 1991 The Warsaw Pact is officially dissolved.
- 1991 The Baltic republics—Latvia, Lithuania, and Estonia—declare their independence and the Soviet Union crumbles. A commonwealth of independent states takes the place of the former Soviet empire. Boris Yeltsin becomes president of Russia.
- 1991 U.S. Navy Fleet Intelligence Center (FIC) Pacific (FICPAC) and FIC Europe-Atlantic (FICEURLANT) absorbed into National Military Joint Intelligence Center (NMJIC).
- 1991 U.S. Army Intelligence Agency ceases to exist; absorbed by Intelligence and Security Command (INSCOM).
- 1991 Lustration law enacted in the Czech Republic, barring persons who had collaborated with the secret police during communist rule from serving in most public posts.
- 1991 In December, Britain's MI5 signals a new era of openness when it announces the appointment of a new director-general, Stella Rimington, the first MI5 chief to be publicly identified.
- 1992 Federal Republic of Yugoslavia collapses; fierce fighting between ethnic groups ensues.
- 1992 The U.S. Army begins collecting blood and tissue samples from all new recruits as part of a "genetic dog tag" program aimed at better identification of soldiers killed in combat.
- 1992 Naval Criminal Investigative Service formed as an entity separate from the Office of Naval Intelligence.
- 1992 In August, DEA creates its Intelligence Division.
- 1992 Land Remote Sensing Policy Act of 1992 establishes legal basis for ownership and operation of commercial remote sensing satellites in the United States.
- 1992 The FBI establishes a Criminal Justice Information Services (CJIS) Division.
- 1992 The United States conducts its last nuclear explosion test in September.
- 1993 Czechoslovakia dissolves into the Czech Republic and Slovakia.
- 1993 The Maastricht Treaty officially forms the European Union.
- 1993 U.S. Congress passes the Domestic Chemical Diversion Control Act, aimed to stop the conversion of legal substances into illegal substances.
- 1993 February 26: the World Trade Center in New York City is badly damaged when a car bomb planted by Islamic terrorists explodes in an underground garage. The bombing leaves six people dead and 1,000 injured. The men carrying out the attack were followers of Umar Abd al-Rahman, an Islamic cleric who preached in the New York City area.
- 1993 After a 51-day siege by the Bureau of Alcohol, Tobacco, and Firearms, federal teams assault a compound held by the Branch Davidians, a religious sect charged with hoarding illegal weapons. The Branch Davidians set the buildings on fire, killing 76 people, including cult leader David Koresh.
- 1993 On April 14, Iraqi intelligence agents attempt to assassinate former president George H.W. Bush during a visit to Kuwait. Two months later, President William J. Clinton launches a cruise missile attack on the Iraqi capital of Baghdad.
- 1993 U.S. Department of Defense closes the Naval Intelligence Command, whose functions—along with those of the Naval Technical Intelligence Center, Task Force 168, and the Navy Operational Intelligence Center—are absorbed by the Office of Naval Intelligence.
- 1993 China defies informal global moratorium on nuclear testing with a weapons test.
- 1993 The final Global Positioning Satellite (GPS) is placed into orbit and the GPS system becomes fully operational.
- 1993 Explosive growth of Internet begins as a result of two factors: the full opening of the National Science Foundation's NSFNET, and the development of the first browsers, Mosaic (forerunner of Netscape Navigator) and Microsoft Internet Explorer.
- 1993 In October, U.S. Air Force Air Intelligence Agency replaces Air Force Intelligence Service.
- 1993 On October 3, 18 U.S. Rangers, participants in a UN peacekeeping force in Somalia, are killed in a firefight on the streets of Mogadishu.
- 1993 In the wake of a congressional ban on the deployment of space-based weapons, the Ballistic Missile

- Defense Organization (BMDO) forms. The collapse of the former Soviet Union makes a large-scale attack upon the United States appear much less likely and Congress seeks to push the DOD to update missile defense programs to address the dangers of the post-Cold War world. In this changed political climate, secretary of defense Les Aspin announces that former president Reagan's ten-year-old Strategic Defense Initiative (popularly known as "Star Wars") will be terminated, with missile defense responsibilities transferred to the newly formed BMDO.
- 1993 *Time* magazine names the personal computer as its "man of the year," as personal computer sales skyrocket, changing the way people around the world work, play and communicate.
- 1994 The Genetic Privacy Act, the first U.S. Human Genome Project legislative product, proposes regulation of the collection, analysis, storage, and use of DNA samples and genetic information. These rules were endorsed by the ELSI Working Group.
- 1994 Aldrich Ames, a 30-year CIA veteran, and his wife, Maria del Rosario Casas Ames, are arrested on espionage charges for selling secrets to the former Soviet Union.
- 1994 Jewish right-wing extremist and U.S. citizen Baruch Goldstein kills Muslim worshippers at a mosque in the West Bank town of Hebron, killing 29 and wounding about 150.
- 1994 North Korea withdraws its membership from IAEA over dispute regarding nuclear inspections.
- 1994 U.S. Navy, Marine, and Coast Guard intelligence agencies begin operating jointly from the National Maritime Intelligence Center in Suitland, Maryland.
- 1994 Congress reduces the lifetime-protection provisions for U.S. presidents, authorizing Secret Service protection only for the first 10 years after leaving office. The new law applies to all presidents in office after January 1, 1997.
- 1994 Britain's Parliament passes Intelligence Services Act, which gives MI6 new statutory grounding. The Act defines the responsibilities and functions of MI6 and its chief, and sets in place a framework of government oversight for MI6 activities.
- 1994 U.S. military action in Haiti restores government of ousted president Jean-Bertrand Aristide.
- 1994 After Rwandan dictator Major General Juvenal Habyarimana dies in a plane crash on April 6, his Hutu supporters blame the Tutsi-controlled Rwandan Patriotic Front, and launch a campaign of genocide that results in more than 800,000 deaths.
- 1994 Russia invades Chechnya on October 11, launching a war that will last almost two years.
- 1995 Combinatorial chemistry, a technique which quickly surveys huge numbers of chemical combinations in order to select the most desirable molecular configurations, attracts the attentions of chemical companies. Scientists predict the possibility of creating numerous new chemicals to serve the needs of industrial and pharmaceutical development, along with defense technology.
- 1995 President Clinton signs Executive Order 12968 on February 22, which provides rules for access to classified information.
- 1995 Study by the Rand Corporation finds that every dollar spent in drug treatment saves society seven dollars in crime, policing, incarceration, and health services.
- 1995 UN Security Council resolution 986 allows partial resumption of Iraqi oil exports, with the original intent to allow Iraq to sell oil to buy food and medicine (the "oil-for-food program"). Iraq subsequently diverts funds from sales to additional weapons purchases and the building of offices and places for the Hussein government. Malnutrition and improper medical care becomes widespread in Iraq.
- 1995 After thwarting UN weapons inspectors, the government of Iraq admits to producing over 8,000 liters of concentrated anthrax as part of the nation's biological weapons program.
- 1995 Twelve are killed and 5,700 injured in a sarin nerve gas attack on a crowded subway station in the center of Tokyo. Aum Shinri-kyu cult is blamed for the attacks.
- 1995 A truck bomb explodes outside the Alfred P. Murrah Federal office building in Oklahoma City, Oklahoma, on April 19, collapsing walls and floors. The massive explosion kills 169, including 19 children and one person who dies in the rescue effort. Timothy McVeigh and Terry Nichols are later convicted in the anti-government plot to avenge the Branch Davidian stand-off in Waco, Texas, exactly two years earlier.
- 1995 Concerned by revelations that agents of the CIA have committed human rights violations in Guatemala, the CIA draws up guidelines prohibiting the agency from hiring agents with records of human-rights violations.
- 1995 June 1995, while Comprehensive Nuclear Test Ban Treaty (CTBT) negotiations are still under way, France announces that it will resume nuclear testing.
- 1995 President Clinton issues Presidential Decision Directive 39, "U.S. Policy on Counterterrorism," calling for a number of specific efforts to deter terrorism in the U.S. as well as attacks on its citizens and allies abroad.
- 1995 Radical Sunni Muslims set off a bomb at a national guard facility in Riyadh, Saudi Arabia, killing five Americans.
- 1995 NATO launches air strikes against Bosnian Serb positions to force the Bosnian Serbs to negotiate a peace settlement. NATO deploys Implementation Force (Ifor) to monitor and enforce a ceasefire.
- 1995 Dayton Accords end fighting in Bosnia.
- 1996 Defense Authorization Act directs Advanced Research Projects Agency (ARPA) to once again be named the Defense Advanced Research Projects Agency (DARPA).
- 1996 An Irish Republican Army (IRA) bomb detonates in London on February 9, killing two persons and wounding more than 100 others, including two U.S. citizens.
- 1996 International participants in the genome project meet in Bermuda and agree to formalize the conditions of

- data access. The agreement, known as the "Bermuda Principles," calls for the release of sequence data into public databases within 24 hours.
- 1996** National Imagery and Mapping Agency (NIMA) created by the consolidation of several existing government and military agencies.
- 1996** The Health Care Portability and Accountability Act incorporates provisions to prohibit the use of genetic information in certain health-insurance eligibility decisions. The Department of Health and Human Services is charged with the enforcement of health-information privacy provisions.
- 1996** U.S. signs the Comprehensive Test Ban Treaty, but the Senate ultimately refuses (in 1999) to ratify the treaty.
- 1996** In an effort to reduce counterfeiting, federal government makes first major change to U.S. currency in 70 years.
- 1996** The Chemical and Biological Incident Response Force (CBIRF), a unit of the U.S. Marines devoted to countering chemical or biological threats at home and abroad, is activated.
- 1996** World chess champion Garry Kasparov, able to compute the ramifications of 2–3 chess moves per second, loses a chess match to IBM's Deep Blue computer, able to compute the ramifications of 200 million moves per second.
- 1996** France conducts its last nuclear weapons test and immediately afterwards French president Jacques Chirac announces his support for a comprehensive test ban.
- 1996** A fuel truck carrying a bomb explodes outside the U.S. military's Khobar Towers housing facility in Dhahran, Saudi Arabia, on June 25, killing 19 U.S. military personnel and wounding 515 persons, including 240 U.S. personnel. Thirteen Saudis and a Lebanese, all alleged members of Islamic militant group Hezbollah, are eventually indicted.
- 1996** China conducts its last nuclear explosion test.
- 1996** Bombing at Atlanta's Centennial Olympic Park on July 27, during the Olympic Games, kills two people and injures 112. Eric Robert Rudolph is charged with the crime, but he evades the authorities until his capture in 2003.
- 1996** Dolphins and sea lions used to protect waters off San Diego during the Republican Party convention.
- 1996** On October 11, President Clinton signs into law the Economic Espionage Act, which makes it a federal crime to use unauthorized means to obtain any trade secret whose transfer to other parties would cause economic harm to its lawful owner.
- 1996** Twenty-three members of the Tupac Amaru Revolutionary Movement (MRTA) take several hundred people hostage at a party given at the Japanese Ambassador's residence in Lima, Peru on December 17. Among the hostages were several U.S. officials, foreign ambassadors and other diplomats, Peruvian Government officials, and Japanese businessmen. The group demanded the release of all MRTA members in prison and safe passage for them and the hostage takers. The terrorists released most of the hostages in December but held 81 Peruvians and Japanese citizens for several months.
- 1996** U.S. Economic Espionage Act passed.
- 1997** Ian Wilmut of the Roslin Institute in Edinburgh, Scotland, announces the birth of a lamb called Dolly, the first mammal cloned from an adult cell, specifically, a cell in a pregnant ewe's mammary gland.
- 1997** The National Center for Human Genome Research (NCHGR) at the National Institutes of Health becomes the National Human Genome Research Institute (NHGRI).
- 1997** U.S. National Cancer Institute estimates that 160 million people in the United States were exposed to some level of iodine 131 from prior U.S. nuclear tests conducted in Nevada, and that these exposures would, over time, cause 30,000–75,000 cases of thyroid cancer.
- 1997** Congress passes the Fair Credit Reporting Act (FCRA), which establishes rights involving records from consumer reporting agencies.
- 1997** Department of Energy creates Chemical and Biological National Security Program to develop systems and technologies to protect civilian populations against the threats associated with chemical, biological, and nuclear attacks.
- 1997** The corrupt regime of Mobutu Sese Seko, a longtime U.S. ally in Zaire, is overthrown by rebel forces under the leadership of Laurent Kabila. Kabila will change the country's name back to Congo, but his regime will bring few democratic reforms, and he will be killed by his own bodyguards in 2001.
- 1997** Tourist killings in Egypt, November 17. Al-Gama'at al-Islamiyya (IG) gunmen shoot and kill 58 tourists and four Egyptians and wound 26 others at the Hatshepsut Temple in the Valley of the Kings near Luxor.
- 1997** The FBI announces its new National DNA Index System (NDIS) on December 8, allowing forensic science laboratories to link serial violent crimes to each other and to known sex offenders through the electronic exchange of DNA profiles.
- 1998** The Hebron Accord, designed to promote peace between Israel and Palestine, is undermined by both sides as terrorism breaks out and the building of new settlements defies non-expansionist agreements.
- 1998** Craig Venter forms a company (later named Celera), and predicts that the company will decode the entire human genome within three years. Celera plans to use a "whole genome shotgun" method, which will assemble the genome without using maps. Venter says that his company will not follow the Bermuda principles concerning data release.
- 1998** DNA analyses of semen stains on a dress worn by White House aide Monica Lewinsky are found to match DNA from a blood sample taken from President Clinton.
- 1998** DNA fingerprinting used to identify remains of Russian Imperial Romanov family.

- 1998 India and Pakistan conduct underground nuclear tests. Exaggerated results are detected using seismic records.
- 1998 Controversy breaks out over the reported NSA Echelon project, which privacy groups describe as a worldwide surveillance network that eavesdrops on communications traffic and shares intelligence gathered by the United States, Great Britain, Canada, Australia and New Zealand.
- 1998 International Atomic Energy Agency Iraq Action Team withdraws from Iraq because of a lack of "full and free access" to Iraqi sites.
- 1998 Congress passes Digital Millennium Copyright Act (DMCA), the most comprehensive overhaul of copyright law in a generation.
- 1998 Presidential Decision Directive 61, issued by President Clinton in February, reorganizes DOE Office of Intelligence.
- 1998 U.S. Army combines its Chemical and Biological Defense Command and Soldier Systems Command to form U.S. Army Soldier and Biological Chemical Command (SBCCOM).
- 1998 Due to heightened concerns over technology leaks from the U.S. Commerce Department to China, commerce secretary William Daley announces plans to tighten security and limit access to classified information within the department.
- 1998 Presidential Decision Directive 63, signed by President Clinton in May, establishes the Critical Infrastructure Assurance Office (CIAO) of the U.S. Department of Commerce.
- 1998 Real IRA explodes a car bomb outside a store in Banbridge, Northern Ireland.
- 1998 U.S. embassy bombings in East Africa, August 7, 1998: A bomb explodes at the rear entrance of the U.S. embassy in Nairobi, Kenya, killing 12 U.S. citizens, 32 foreign service workers, and 247 Kenyan citizens. About 5,000 Kenyans, six U.S. citizens, and 13 foreign service workers are injured. Almost simultaneously, a bomb detonates outside the U.S. embassy in Dar es Salaam, Tanzania, killing seven foreign service workers and three Tanzanian citizens, and injuring one U.S. citizen and 76 Tanzanians. The U.S. government holds Osama Bin Laden responsible.
- 1998 Formation, in October, of the U.S. National Domestic Preparedness Office as the coordination center for all federal efforts in response to weapons of mass destruction.
- 1998 Digital Millennium Copyright Act (DMCA) passed.
- 1998 Iraq expels UN weapons inspectors on October 31. In December, the United States and Britain launch Operation Desert Fox to attempt to destroy Iraq's nuclear, chemical, and biological weapons programs.
- 1999 Vladimir Putin becomes prime minister of Russia.
- 1999 The Czech Republic, Hungary, and Poland become the first former Soviet bloc states to join NATO, taking the alliance's borders some 400 miles towards Russia.
- 1999 President Clinton signs Executive Order 13142, which amends Executive Order 12958 by extending the period of classification for some sensitive documents.
- 1999 Taiwanese-born computer scientist Wen Ho Lee is fired from his job in March and subsequently arrested by the FBI. Charged with not properly securing classified materials and failing to report meetings with individuals from "sensitive" countries, Lee will be held for a year and eventually convicted in 2000.
- 1999 Beginning March 24, NATO forces conduct a 78-day campaign of air strikes to end Serb "ethnic cleansing" in the Albanian enclave of Kosovo and to break the hold of Serbian leader Slobodan Milosevic.
- 1999 Melissa virus (actually a form of malicious data wedded to a particular type of virus program, a macro virus) spreads through the e-mail systems of the world on March 26, causing \$80 million worth of damage, primarily in the form of lost productivity resulting from the shutdown of overloaded mailboxes.
- 1999 Osama bin Laden is added to the FBI's Ten Most Wanted Fugitives list in June, in connection with the U.S. embassy bombings in eastern Africa.
- 1999 FBI personnel travel to Kosovo on June 23 to assist in the collection of evidence and the examination of forensic materials in support of the prosecution of Slobodan Milosevic and others before the International Criminal Tribunal for the former Yugoslavia.
- 1999 Congress releases a bipartisan report asserting that China stole nuclear secrets regarding U.S. weapons. The systematic espionage campaign by the Chinese is alleged to date to the 1970s.
- 1999 A nuclear accident at Japan's Tokaimura facility occurs on September 30 when a criticality event, or unplanned chain reaction, exposes 39 workers to radiation contamination and causes the evacuation of families within 350 meters of the facility.
- 1999 Russia invades Chechnya on October 1, resuming hostilities that had abated since 1996.
- 1999 IKONOS, the world's first commercial remote sensing satellite with 1 meter resolution, is launched.
- 1999 UN Security Council resolution 1284 creates the UN Monitoring, Verification and Inspection Commission (UNMOVIC) as a replacement for UNSCOM. Saddam Hussein rejects the resolution. In March 2000, Hans Blix becomes chairman of UNMOVIC.
- 1999 A merger of the ACDA and U.S. State Department creates a number of new bureaus, including the Bureau of Arms Control.
- 1999 As the year 2000 approaches, the world prepares itself for the possible deleterious effects of a computer shortcut (a protocol developed when memory was scarce) that used only the last two digits of a year to indicate the year. Termed the Y2K problem, fears approach near hysteria as people and governments prepare for computers to malfunction and adversely affect critical infrastructure. Adequate preparation, considerable investment in programming solutions,

- and monitoring turn the dawn of 2000 into a grand worldwide party but a non-event with regard to Y2K fears. Minimal disruptions are reported.
- 2000** Mokhtar Haouari and Abdel Ghani Meskini are charged with collaborating with Ahmed Ressam and others in a wide-ranging terrorist conspiracy to bomb U.S. sites during the January 1, 2000, millennium celebrations. The FBI/New York Police Department Joint Terrorist Task Force, Royal Canadian Mounted Police, the Canadian Security and Intelligence Service, and Canada's Department of Justice collaborate in the investigation.
- 2000** Islamic extremist group Asbat al-Ansar carries out a rocket-propelled grenade attack on the Russian embassy in Beirut in January 2000.
- 2000** The Jaish-e-Mohammed, an Islamic extremist group based in Pakistan, is formed by Masood Azhar upon his release from prison in India in early 2000.
- 2000** President Clinton signs an executive order prohibiting federal departments and agencies from using genetic information in hiring or promoting workers.
- 2000** NNSA begins operations on March 1, 2000. NNSA has the mission of improving national security through defense uses of nuclear energy.
- 2000** Beginning in October, OIS divides its functions between its Information Security Services Center and its new Office of Information Assurance and Critical Infrastructure Protection.
- 2000** October 12, terrorist bombing of USS *Cole* kills 17 of its crew and wounds 39 others. Two suicide bombers, ultimately linked to al-Qaeda, pull alongside the vessel near the port in Aden, Yemen, and detonate explosives near the *Cole's* hull.
- 2000** The PLO's terrorist campaign against Israel again intensifies with start of a second Intifada.
- 2000** Former U.S. senator John Danforth, conducting an independent review of FBI actions in the 1993 FBI assault on the Branch Davidian compound in Waco, Texas, releases his final report exonerating the FBI of wrongdoing. The Government Operations Committee reaches a similar conclusion.
- 2001** On January 5, just 15 days before leaving office, President Clinton issues Presidential Decision Directive (PDD) 75, "U.S. Counterintelligence Effectiveness—Counterintelligence for the Twenty-first Century."
- 2001** A U.S. Navy P-3 on a surveillance mission over the South China Sea collides with a Chinese fighter plane, killing the Chinese pilot and forcing the American plane to make an emergency landing on China's Hainan Island. Although the Chinese pilot is blamed for the collision, Washington issues "regrets" but no apology (as is demanded by the Chinese) to secure the release of the U.S. crew after they are held for 11 days.
- 2001** The FBI announces on January 5 the National InfraGuard program at the FBI's National Infrastructure Protection Center. The program centers on securely sharing information about computer intrusions and intrusion threats between business and law enforcement so that the confidentiality of potentially affected businesses is protected.
- 2001** The complete draft sequence of the human genome is published in February. The public sequence data is published in the British journal *Nature* and the Celera sequence is published in the American journal *Science*. Increased knowledge of the human genome allows greater specificity in pharmacological research and drug interaction studies.
- 2001** FBI Agent Robert Philip Hanssen is arrested on February 18 for conspiracy to commit espionage. The affidavit in support of an arrest warrant for Hanssen charges that he engaged in a lengthy relationship with the KGB and its agencies.
- 2001** Following years of Iraqi firings upon U.S. and British airplanes patrolling the northern and southern "no fly" zones, the United States and Britain carry out bombing raids in February with the intent to disable Iraq's air defense network.
- 2001** President George W. Bush presents the Congressional Gold Medal to World War II Navajo code talkers (windtalkers).
- 2001** In May, Libyan leader Muammar Qaddafi admits to a German newspaper that Libya was behind a Berlin discotheque bombing in 1986 that killed a U.S. serviceman and a Turkish civilian, and injured some 200 others. At a trial in November, four defendants are convicted for roles in the bombing.
- 2001** Hamas claims responsibility for the bombing of a popular Israeli nightclub that causes more than 140 casualties.
- 2001** A U.S. grand jury indicts fourteen Hezbollah members on June 21 for the 1996 Khobar Towers bombing.
- 2001** Ahmad Shah Massoud, the leader of the rebels in the Afghanistan Northern Alliance, widely regarded as the most popular opposition figure to the ruling Taliban (the regime providing asylum to al-Qaeda and its leader, Osama bin Laden) is assassinated on September 9.
- 2001** September 11, Islamist terrorists mount coordinated attacks on New York and Washington. The World Trade Center towers are destroyed, killing nearly 3,000 people. In Washington, a plane slams into the Pentagon, while passengers aboard another hijacked airliner, aware of the other terrorist attacks, fight back. During the struggle for the aircraft, it crashes into a Pennsylvania field, thwarting the terrorists' plans to crash the plane into either the U.S. Capitol or the White House. The FBI dedicates 7,000 of its 11,000 special agents and thousands of FBI support personnel to the PENTTBOM investigation. "PENTTBOM" is short for Pentagon, Twin Towers Bombing.
- 2001** Letters containing a powdered form of *Bacillus anthracis*, the bacteria that causes anthrax, are mailed by an unknown terrorist or terrorist group (foreign or domestic) to government representatives, members of the news media, and others in the United States. More than 20 cases and five deaths are eventually attributed to the terrorist attack.

- 2001 On October 7, United States launches Operation Enduring Freedom against the al-Qaeda terror network and Afghanistan's Taliban regime. The Taliban regime is toppled and many al-Qaeda operatives are killed, but Osama bin Laden evades capture.
- 2001 Following the September 11 attacks, NATO secretary-general George Robertson invokes Article Five of the alliance's constitution, which states that an attack on one member nation is seen as an attack on all. Washington chooses, however, not to involve NATO in the U.S.-led military campaign which follows.
- 2001 QuickBird satellite launched, providing sub meter commercial satellite images.
- 2001 On October 16, President Bush signs Executive Order 13231, "Critical Infrastructure Protection in the Information Age."
- 2001 On October 26, President Bush signs the USA Patriot Act into law, giving the FBI and CIA broader investigatory powers and allowing them to share confidential information about suspected terrorists with one another. Under the act, both agencies can conduct residential searches without a warrant and without the presence of the suspect and immediately seize personal records. The provisions are not limited to investigating suspected terrorists, but may be used in any criminal investigation related to terrorism. The Patriot Act also grants the FBI and CIA greater latitude in using computer tracking devices such as the Carnivore (DCS1000) to gain access to Internet and phone records.
- 2001 Disarmament operations begin in the former Yugoslav republic of Macedonia.
- 2001 Chernobyl nuclear power plant begins decommissioning.
- 2001 In *United States v. Scarfo*, a federal judge in Newark, New Jersey, grants the government's motion to suppress information on an FBI computer keystroke recording device under the Classified Information Protection Act (CIPA).
- 2001 Fourth Marine Expeditionary Brigade formed. It consists of the Marine Security Force Battalion, the Marine Security Guard Battalion, the Chemical and Biological Incident Response Force, and the new anti-terrorism battalion. The latter had evolved from the 1st Battalion, 8th Marines, which had been hit in the 1983 bombings of U.S. Marine barracks in Lebanon.
- 2001 On November 19, President George W. Bush signs into law the Aviation and Transportation Security Act (ATSA), which creates the Transportation Security Administration (TSA), and authorizes TSA to direct a team of air marshals and federal airport security screeners.
- 2001 United Kingdom passes a new counter-terrorist bill in December, the Anti-Terrorism, Crime, and Security Act. The act allows British authorities to detain suspected terrorists for up to six months before reviewing their cases and for additional six-month periods after that. As in the United States, civil liberty advocate groups in the United Kingdom criticize the new law for potentially infringing upon a basic civil liberty, specifically the right to avoid unlawful detention and gain access to a speedy trial.
- 2001 The Chemical and Biological Incident Response Force (CBIRF) sends a 100-member initial response team into the Dirksen Senate Office Building in Washington on December 2 alongside EPA specialists to detect and remove anthrax spores which had been introduced into the building in a letter. A similar mission was undertaken at the Longworth House Office Building in October, during which time samples were collected from more than 200 office spaces.
- 2001 FBI Director Mueller orders the reorganization of FBI operations on December 3 to respond to a revised agency mission that emphasizes terrorism prevention and internal accountability, and strengthens partnerships with domestic and international law enforcement.
- 2001 Enough closed-circuit television cameras (CCTV) are installed in public places in Britain that, on an average day in any large British city, security experts calculate that a person will have over 300 opportunities to be captured on CCTV during the course of normal daily activities.
- 2001 U.S. unmanned plane completes trans-Pacific flight from California to Australia.
- 2001 Brian Regan, retired U.S. Air Force master sergeant and cryptanalyst, is arrested on charges of spying for Iraq, Libya and China.
- 2002 In the aftermath of the September 11 attacks, the U.S. government dramatically increases funding to stockpile drugs and other agents that could be used to counter a bioterrorism attack.
- 2002 An explosives-laden boat rams the French oil tanker *Limburg* off the coast of Yemen, killing one member of the tanker's crew, tearing a hole in the vessel and spilling 90,000 barrels of oil. U.S. experts believe that the attack was perpetrated by al-Qaeda members.
- 2002 Industrialized nations pledge \$10 billion to help Russia secure Soviet era nuclear weapons and materials.
- 2002 The planned destruction of stocks of smallpox-causing Variola virus at the two remaining depositories in the United States and Russia is delayed over fears that large-scale production of vaccine might be needed in the event of a bioterrorist action.
- 2002 More than 1,300 FBI personnel, along with representatives of other federal, state, and local law enforcement agencies, ensure safety at the 2002 Winter Olympic Games in Salt Lake City. Preparations for the games began in May 1998 and included multiple training exercises involving weapons of mass destruction scenarios.
- 2002 Scientists at Russia's DS Likhachev Scientific Research Institute for Cultural Heritage and Environmental Protection successfully breed a new kind of highly efficient explosives sniffer dog. The new breed is a cross between a jackal and a Russian Husky.
- 2002 The Pathogen Genomic Sequencing program is initiated by DARPA to focus on characterizing the genetic components of pathogens in order to develop

- diagnostics, treatments and therapies for the diseases they cause.
- 2002 GAO reports that 13 of the hijackers involved in the September 11 attacks had not been interviewed by U.S. consular officials prior to the granting of visas.
- 2002 DARPA initiates the Biosensor Technologies program in 2002 to develop fast, sensitive, automatic technologies for the detection and identification of biological warfare agents.
- 2002 A report released in March by the U.S. National Academy of Sciences Institute of Medicine concludes that AVA anthrax vaccine is “acceptably safe.”
- 2002 Russian and NATO foreign ministers reach final agreement in May on the establishment of the NATO-Russia Council, in which Russia and the 19 NATO countries will have an equal role in decision-making on policy to counter terrorism and other security threats.
- 2002 NATO secretary-general George Robertson visits Ukrainian capital in July and welcomes Ukraine’s declared desire for membership, but he states that further political, economic, and military reforms are necessary before Ukraine can join.
- 2002 The United States withdraws from the ABM treaty in July.
- 2002 President Bush calls upon the UN to confront the Iraqi threat and usurp potential Iraqi transfer of weapons of mass destruction to terrorist groups.
- 2002 On October 1, the U.S. Strategic Command and U.S. Space Command merge to form USSTRATCOM, located at Offutt Air Force Base in Nebraska.
- 2002 Under threat of serious consequences, including potential military action based on UN Resolution 1441, Iraq allows IAEA’s Iraq Action Team to resume inspections in Iraq. The Iraq Action Team is renamed the Iraq Nuclear Verification Office (INVO).
- 2002 London police arrest seven men in connection with ricin manufacture.
- 2002 On November 26, President Bush signs into law the Terrorism Risk Insurance Act, intended to cover the private sector in the event of terrorist attacks such as those that occurred on September 11.
- 2002 Seven countries—Lithuania, Estonia, Latvia, Bulgaria, Romania, Slovakia and Slovenia, are invited to join the European Union at a summit meeting in Prague.
- 2002 Congress passes and President Bush signs the Homeland Security Act of 2002 into law creating the Department of Homeland Security.
- 2002 In November, a CIA-operated Predator drone fires a missile that kills Osama bin Laden’s top lieutenant in Yemen, Qaed Salim Sinan al-Harethi, and five other al-Qaeda suspects.
- 2002 A group of Swiss researchers at the Lausanne-based Dalle Molle Institute for Perceptual Artificial Intelligence claim they are 95 percent certain that a tape purported to show Osama Bin Laden and played on Arabic television network Al-Jazeera was a fake. U.S. officials continue to assert that the tape is probably genuine. Investigators claim that the poor tape quality defeats sophisticated efforts using aural spectrogram machines that rely on biometric algorithms to analyze breath patterns, syllable emphasis, frequency of speech, rate of speech, and other factors. Over the next several months, additional tapes are released with experts generally agreeing only that the voice alleged to be that of bin Laden could be genuine. The authenticity of the tapes was critical to determine if the al-Qaeda leader had survived the U.S. war against al-Qaeda in Afghanistan.
- 2002 Abd al-Rahim al-Nashiri—alleged to be leader of al-Qaeda operations in the Persian Gulf—is captured. Nashiri, also known as Abu Asim al-Makki, is suspected of masterminding the October 2000 attack on the USS *Cole*.
- 2002 Anas al-Liby, one of the FBI’s most-wanted fugitives, is captured in Afghanistan. Al-Liby was allegedly linked to the 1998 bombings of American embassies in Kenya and Tanzania.
- 2002 Ramzi Binalshibh, allegedly one of the most senior al-Qaeda members, is arrested in Pakistan.
- 2002 Trial of Mounir al-Motassadek begins in Germany. Al-Motassadek, a Moroccan, is the first man to stand trial in the September 11 attacks and is charged with being an accessory to more than 3,000 murders in New York and Washington, and of belonging to an al-Qaeda cell in Hamburg. Motassadek claims he knew the hijackers, but only socially; he is convicted and sentenced to 15 years in prison for being a co-conspirator.
- 2002 Zacarias Moussaoui, a 34-year-old French citizen of Moroccan origin, is charged with six counts of conspiracy and faces a possible death sentence for alleged involvement in the September 11 attacks. Moussaoui is referred to as the “20th hijacker”; it is suspected that he was unable to participate in the mission because he had been placed under arrest on an unrelated charge. Moussaoui denies involvement in the attacks but admits to being a member of the al-Qaeda network and at his trial publicly supports the actions of the terrorists.
- 2002 In December, North Korea expels IAEA inspectors, removes surveillance equipment from nuclear facilities, and announces an intent to make plants operational.
- 2003 Office of Homeland Security becomes Department of Homeland Security on January 24.
- 2003 President Bush announces formation of Project BioShield during his 2003 State of the Union Address.
- 2003 Scientists at Sandia National Laboratory report achieving limited controlled fusion using a pulsed power source.
- 2003 North Korea pulls out of the Treaty on the Non-Proliferation of Nuclear Weapons (NPT).
- 2003 U.S. secretary of state Colin L. Powell presents to the UN Security Council evidence of Iraq’s continued development of prohibited biological weapons.
- 2003 NATO’s internal divisions are highlighted as France, Germany, and Belgium temporarily block U.S. moves

- to offer military support to Turkey in the event of war in Iraq.
- 2003** Ten suspected terrorists mysteriously vanish from a high-security prison in Yemen. Among the escapees are two top suspects in the bombing of the USS *Cole*.
- 2003** Richard Reid, the “shoe bomber” who attempted a suicide bombing of an American Airlines Paris-to-Miami flight in December 2001, pleads guilty on all eight charges against him and declares himself a follower of Osama bin Laden. Reid is sentenced to life in prison without possibility of parole.
- 2003** U.S. government officials claim that the capture of top al-Qaeda lieutenant Khalid Sheik Mohammed, allegedly al-’s chief operations planner, also yields valuable documents and computer files outlining al-Qaeda operations.
- 2003** August 19: a truck-bomb explodes near the UN Iraq headquarters in Baghdad, killing 17, including Sergio Vieira de Mello, head of the UN delegation in Iraq.
- 2003** Virtually all agencies scheduled for transfer to the new Department of Homeland Security are officially moved in a March 1 ceremony attended by President Bush.
- 2003** Break-up of the space shuttle *Columbia* upon reentry. Scientists use GIS technology to map debris field.
- 2003** Carbon-graphite coils capable of generating an electromagnetic pulse or otherwise disabling electronics are used in U.S.-led raids on Baghdad, Iraq.
- 2003** Dolphins and sea lions used in mine detection and swimmer defense in waters off of Iraq.
- 2003** U.S. intelligence sources indicate that at least 17 nations around the globe have offensive biological weapons programs.
- 2003** On March 17, U.S. president Bush gives Saddam Hussein and his sons 48 hours to leave Iraq or face war. On March 20, American missiles hit “targets of opportunity” in Baghdad, marking the start of the war to oust Hussein. Intelligence sources on the ground in Iraq have indicated that Hussein and other elements of the Iraqi leadership are meeting in a bunker in Baghdad. In less than 45 minutes, a U.S. B-2 stealth bomber armed with “bunker-buster” munitions attempts to eliminate the Iraqi leadership. For several weeks the fate of Hussein is debated, with Iraqi television showing images of Hussein that do not definitively verify his survival. Within days, U.S. and British ground troops enter Iraq from the south, and on April 9, U.S. forces advance into central Baghdad. Hussein government is toppled, but U.S. efforts to establish order and a new government are hampered by sporadic attacks and sectarian violence.
- 2003** PLF leader Abu Abbas, found guilty of the murder of an elderly American during the 1985 terrorist hijacking of the cruise ship *Achille Lauro*, is discovered and arrested in Baghdad following Operation Iraqi Freedom.
- 2003** UN Security Council approves resolution backing the U.S.-led administration in Iraq and plan to lift economic sanctions. U.S. administrator abolishes the Baath Party and security institutions of Saddam Hussein’s regime.
- 2003** August 19: a truck-bomb explodes near the UN Iraq headquarters in Baghdad, killing 17, including Sergio Vieira de Mello, head of the UN delegation in Iraq.
- 2003** September 23: two U.S. military personnel who have been working at the Guantanamo Bay, Cuba, detention facility, where suspected al-Qaeda members are being held, are accused of espionage.



*This page intentionally left blank*

# Sources

## Books

- 15 Years of Serving the President, 1982–1997. Washington, D.C.: National Security Telecommunications Advisory Committee, 1997.
- 200th Anniversary of the Office of the Attorney General, 1789–1989. Washington, D.C.: Department of Justice, 1991.
- A Cold War Conundrum: The 1983 Soviet War Scare. Washington, D.C.: Center for the Study of Intelligence, 1997.
- Abanes, Richard. *American Militias: Rebellion, Racism, and Religion*. Downers Grove, IL: InterVarsity Press, 1996.
- Abbott, Patrick. *Airship*. New York: Charles Scribner's Sons, 1973.
- Ackerman, S. *Discovering the Brain*. National Academy Press, 1992.
- Ackermann, U. *Essentials of Human Physiology*. St. Louis: Mosby Year Book, Inc., 1992.
- Adams, Herbert F. R. *SI Metric Units: An Introduction*. Toronto: McGraw-Hill Ryerson, 1974.
- Adams, James L. *Flying Buttresses, Entropy, and O-Rings: The World of an Engineer*. Cambridge: Harvard University Press, 1991.
- Adams, John A. *Dirt*. College Station, TX: Texas A&M University Press, 1986.
- Adams, Raymond D., and Maurice Victor. *Principles of Neurology*. New York: McGraw-Hill, 1989.
- Adams-Deschamps, Helene. *Spyglass: An Autobiography*. New York: Holt, 1995.
- Aebi, Engel. *Atlas of Microscopy Techniques*. San Diego: Plenum Press, 2002.
- Agutter P.S. *Between Nucleus and Cytoplasm*. New York: Chapman and Hall, 1991.
- Aharoni, Zvi. Also with: Wilhelm Dietl, Meir Amit, and Helmut Bogler (trans.) *Operation Eichmann: The Truth About the Pursuit, Capture and Trial*. New York: John Wiley and Sons, 1997.
- Ahrens, C. David, Rachel Alvelais, and Nina Horne. *Essentials of Meteorology: An Invitation to the Atmosphere*. Belmont, CA: Brooks/Cole, 2000.
- Ahrens, C. Donald. *Meteorology Today*. 2d ed. St. Paul, MN: West Publishing Company, 1985.
- Ainsworth, Peter B. *Offender Profiling and Crime Analysis*. Portland, OR: Willan, 2001.
- Akin, Thomas. *Hardening Cisco Routers*. Sebastopol, CA: O'Reilly, 2002.
- Albers, Vernon. *The World of Sound*. Cranbury, NJ: A. S. Barnes and Co., Inc., 1970.
- Albert, A.Z. *Quantum Mechanics and Experience*. Cambridge, MA: Harvard University Press, 1992.
- Alberts, B., D. Bray, J. Lewis, M. Raff, K. Roberts, and J. Watson, eds. *Molecular Biology of the Cell*. 3d ed. New York: Garland Publishing, 1994.
- Alberts, Bruce, Alexander Johnson, Julian Lewis, et al. (eds.) *Molecular Biology of the Cell*. New York: Garland Publishing, 2002.
- Alderman, Ellen, and Caroline Kennedy. *The Right to Privacy*. New York: Knopf, 1995.
- Aldrich, Richard J. *Intelligence and the War Against Japan: Britain, America, and the Politics of Secret Service*. New York: Cambridge University Press, 2000.
- Aldrich, Richard J. *The Hidden Hand: Britain, America, and Cold War Secret Intelligence*. Woodstock, NY: Overlook Press, 2002.
- Aleksander, Igor, and Piers Burnett. *Reinventing Man: The Robot Becomes Reality*. New York: Holt, Rinehart and Winston, 1983.
- Alexander, John B. *Future War: Non-Lethal Weapons in Twenty-First Century Warfare*. New York: St. Martin's Press, 1999.
- Alexander, Martin S. *Knowing Your Friends: Intelligence Inside Alliances and Coalitions from 1914 to the Cold War (Cass Series-Studies in Intelligence)*. London; Portland, OR: Frank Cass, 1998.
- Alexander, Yonah, and Michael S. Swetnam. *Cyber Terrorism*. Ardsley, NY: Transnational, 2001.
- Allen, Edward. *Fundamentals of Building Construction*. 3rd ed. New York, NY: John Wiley & Sons, 1998.
- Allen, Edward. *The Architect's Studio Companion*. 3rd ed. New York, NY: John Wiley & Sons, 2001.

- Allen, G. D., C. Chui, and B. Perry. *Elements of Calculus*. 2nd ed. Pacific Grove, CA: Brooks/Cole Publishing Co., 1989.
- Allen, Garland E., William E. Castle, Charles C. Gillispie, eds. *Dictionary of Scientific Biography*, vol. 3, New York: Scribner, 1971.
- Allen, George W. *None So Blind: A Personal Account of the Intelligence Failure in Vietnam*. Chicago: Ivan R. Dee, 2001.
- Allen, Oliver E., and the Editors of Time-Life Books. *Planet Earth: Atmosphere*. Alexandria, VA: Time-Life Books, 1983.
- Allen, T., and N. Polmar. *Merchants of Treason*. New York: Delacorte Press, 1988.
- Alperin, Jonathan. "Groups and Symmetry." In *Mathematics Today*, edited by Lynn Arthur Steen. New York: Springer-Verlag, 1978.
- Alvarez, David J. *Allied and Axis Signals Intelligence in World War II*. Portland, OR: F. Cass, 1999.
- Alves, Péricles Gasparini. *Prevention of an Arms Race in Outer Space*. New York: United Nations Institute for Disarmament Research, 1991.
- Amend, John R., Bradford P. Mundy, and Melvin T. Arnold. *General, Organic and Biological Chemistry*. Philadelphia: Saunders, 1990.
- American Men and Women of Science: A Biographical Directory of Today's Leaders in Physical, Biological, and Related Sciences, 1998–99*, 20th ed. New Providence, NJ: R.R. Bowker, 1998.
- American National Standard for Information Sciences: Codes for the Representation of Languages for Information Interchange*. National Information Standards Organization, 1991.
- American Psychiatric Association. *Let's Talk about Psychiatric Drugs*. Washington, DC: American Psychiatric Association, 1993.
- American Water Works Association. *Water Quality and Treatment*. 5th ed. Denver: American Water Works Association, 1999.
- An Overview of the Emergency Response Program*. Washington, D.C.: U.S. Environmental Protection Agency, 1992.
- Anastasi, A. *Psychological Testing*. New York: Macmillan, 1982.
- Anch, A. Michael et al. *Sleep: A Scientific Perspective*. Englewood Cliffs, NJ: Prentice Hall, 1988.
- Anderson, Edwin P. and Rex Miller. *Electric Motors*. New York: Macmillan, 1991.
- Anderson, John D. Jr. *Introduction to Flight*. New York: McGraw-Hill, 1989.
- Anderson, Malcolm. *Policing the World: Interpol and the Politics of International Police Co-operation*. Oxford: Clarendon Press, 1989.
- Anderson, Malcolm. *Policing the World: Interpol and the Politics of International Police Co-operation*. Oxford: Clarendon Press, 1989.
- Andreason, N.C., and D.W. Black. *Introductory Textbook of Psychiatry*. Washington, DC: American Psychiatric Press, Inc., 1991.
- Andreoli, Thomas E. et al. *Cecil Essentials of Medicine*. Philadelphia: W.B. Saunders Company, 1993.
- Andrew, C. *For the President's Eyes Only-Secret Intelligence and the American Presidency from Washington to Bush*. New York: Harper Collins Publishers, 1995.
- Andrew, C., and V. Mitrokhin. *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB*. New York: Basic Books, 1999.
- Andrew, Christopher M. *Codebreaking and Signals Intelligence*. Totowa, NJ: F. Cass, 1986.
- Andrew, Christopher M. *Her Majesty's Secret Service: The Making of the British Intelligence Community*. New York: Viking, 1986.
- Anthony E. Sale, 'The Colossus of Bletchley Park—The German Cipher System', in Raúl Rojas and Ulf Hashagen *The First Computers: History and Architectures*, Cambridge, Massachusetts, MIT Press, 2000.
- Arms, Karen, and Pamela S. Camp. *Biology*. 3rd ed. Philadelphia: Saunders College Publishing, 1987.
- Armstead, Christopher H., ed. *Geothermal Energy*. Paris: UNESCO, 1973.
- Aronstein, David C., and Albert C. Piccirillo. *Have Blue and the F-117A: Evolution of the "Stealth Fighter."* Reston, VA: American Institute of Aeronautics and Astronautics, 1997.
- ARRL. *The Satellite Experimenter's Handbook*. Radio Society of Great Britain: American Radio Relay League, 1990.
- Arson, Ron. *Calculus With Analytic Geometry*. Boston: Houghton Mifflin College, 2002.
- Ashbourn, Julian. *Advanced Identity Verification. The Complete Guide*. London: Springer Verlag, 2000.
- Asimov, Isaac, and Karen A. Frenkel. *Robots: Machines in Man's Image*. New York: Harmony Books, 1985.
- Asimov, Isaac. *Asimov's Biographical Encyclopedia of Science & Technology*. 2nd revised edition. Garden City, NY: Doubleday & Company, Inc., 1982.
- Asimov, Isaac. *Asimov's Chronology of Science and Discovery*. New York: Harper & Row, Publishers, 1989.
- Asimov, Isaac. *Understanding Physics: Light, Magnetism, and Electricity*. Vol. 2. Signet Science Series. New York: NAL, 1969.
- Astor, Gerald. *The "Last" Nazi: The Life and Times of Dr. Joseph Mengele*. New York: Fine, 1985.
- Atherly, A.G., J.R. Girton, and J.F. McDonald. *The Science of Genetics*. Fort Worth, TX: Saunders College Publishing, 1999.
- Atherton, J.C., and M.J. Blaser, eds. "Helicobacter Infections." *Harrison's Principles of Internal Medicine*. New York: McGraw-Hill, 1998.
- Atherton, Louise. *SOE Operations in Africa and the Middle East: A Guide to Newly Released Records in the Public Record Office*. London: PRO Publications, 1994.
- Atherton, Louise. *SOE Operations in Scandinavia: A Guide to the Newly Released Records in the Public Record Office*. London: PRO Publications, 1994.
- Atherton, Louise. *SOE Operations in the Far East: An Introductory Guide to the Newly Released Records of the Special Operations Executive in the Public Record Office*. London: PRO Publications, 1993.
- Atherton, Louise. *Top Secret: An Interim Guide to Recent Releases of Intelligence Records at the Public Record Office*. London: PRO Publications, 1993.
- Atkins, P. *Quanta: A Handbook of Concepts*. Oxford: Oxford University Press, 1991.

- Atkins, P.W. *Molecular Quantum Mechanics*, 2nd ed. Oxford: Oxford University Press, 1983.
- Atkins, P.W. *Molecules*. W. H. Freeman, 1987.
- Atkins, P.W. *Physical Chemistry*, 6th ed. Oxford: Oxford University Press, 1997.
- Atkins, P.W. and J. A. Beran. *General Chemistry*, 2nd edition. New York: Scientific American Books, 1992.
- Atkins, Peter W. *The Second Law*. New York: Freeman, 1984.
- Atkinson, D.E. *Cellular Energy Metabolism and Its Regulation*. New York: Academic, 1977.
- Atkinson, R.L., R.C. Atkinson, E.E. Smith, and D.J. Bem. *Introduction to Psychology*. 10th ed. New York: Harcourt Brace Jovanovich, 1990.
- Atlas, R.M. and R. Bartha. *Microbial Ecology*. Menlo Park, CA: Benjamin/Cummings, 1987.
- Aubrac, Lucie. Konrad Bieber and Betsy Wing (trans.). *Outwitting the Gestapo*. Lincoln, NB: University of Nebraska Press, 1994.
- Ayres, Julia. *Printmaking Techniques*. New York: Watson-Guption, 1993.
- Azaroff, Leonid V. *Elements of X-Ray Crystallography*. New York: McGraw-Hill Book Company, 1968.
- Babington-Smith, Constance. *Evidence in Camera: The Story of Photographic Intelligence in World War II*. Newton Abbott, England: David and Charles, 1974.
- Babiuk, Lorne A., and John J. Phillips, eds. *Animal Biotechnology*. New York: Pergamon Press, 1989.
- Bailey, Brian J. *The Luddite Rebellion*. New York: New York University Press, 1998.
- Bailey, James E. *Ullmann's Encyclopedia of Industrial Chemistry*. New York: VCH, 2003.
- Bailey, Kathleen C. *Iraq's Asymmetric Threat to the United States and U.S. Allies*. Fairfax, VA: National Institute for Public Policy, 2001.
- Bailey, Philip S., Jr., and Christina A. Bailey. *Organic Chemistry: A Brief Summary of Concepts and Applications*. 4th ed. Englewood Cliffs, NJ: Prentice Hall, 1989.
- Ball, Desmond. *Politics and Force Levels: The Strategic Missile Program of the Kennedy Administration*. Lexington: University Press of Kentucky, 1988.
- Ball, W.W. Rouse. *A Short Account of the History of Mathematics*. London: Sterling Publications, 2002.
- Bamford, James. *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency: from the Cold War through the Dawn of a New Century*. New York: Doubleday, 2001.
- Bamford, James. *The Puzzle Palace: A Report on America's Most Secret Agency*. Boston: Houghton, Mifflin, 1982.
- Bancroft, Mary. *Autobiography of a Spy*. New York: Morrow, 1983.
- Banfield, Edwin. *Barometers: Aneroid and Barographs*. Trowbridge, Wiltshire, England: Baros Books, 1985.
- Banks, J. Houston. *Elements of Mathematics*. Allyn and Bacon, 1961.
- Bar-Joseph, Uri. *Intelligence Intervention in the Politics of Democratic States: The United States, Israel, and Britain*. University Park: Pennsylvania State University Press, 1995.
- Barash, Paul G., Bruce F. Cullen, and Robert K. Stoelting. *Clinical Anesthesia*. Philadelphia, Lippincott, 1992.
- Barnes, J. *Basic Geological Mapping*, 3rd ed. New York, John Wiley and Sons, 1995.
- Barnett, Raymond & Michael Ziegler. *College Mathematics*. San Francisco: Dellen Publishing Co, 1984.
- Baron, Paul A., and Klaus Willeke. *Aerosol Measurement: Principles, Techniques, and Applications*. 2nd ed. Hoboken, NJ: Wiley-Interscience, 2001.
- Barrett, E. C., and L. F. Curtis. *Introduction to Environmental Remote Sensing*. New York: Chapman & Hall, 1992.
- Barrett, James T. *Textbook of Immunology*. St. Louis: Mosby, 1988.
- Barron, James W., Morris H. Eagle, and David L. Wolitzky, eds. *Interface of Psychoanalysis and Psychology*. Washington, D.C.: American Psychological Association, 1992.
- Barron, John. *Breaking the Ring*. Boston: Houghton Mifflin, 1987.
- Bates, Robert L. *Industrial Minerals: How They Are Found and Used*. Hillside, NJ: Enslow Publishers, Inc., 1988.
- Bath, Alan Harris. *Tracking the Axis Enemy: The Triumph of Anglo-American Naval Intelligence*. Lawrence, Kansas: University Press of Kansas, 1998.
- Battan, Louis J. *Fundamentals of Meteorology*. Englewood Cliffs, NJ: Prentice-Hall, Inc., 1979.
- Beale, Stephen. *Web Tricks and Techniques: Photo Manipulation: Fast Solutions for Hands-On Web Design*. Gloucester: Rockport Publishers, 2002.
- Bechthold, W. et al. *Direct Disposal of Spent Nuclear Fuel (Radioactive Waste Management Series)*. Graham & Trotman, 1988.
- Becker, W., and D. Deamer. *The World of the Cell*. 2nd ed. New York: Benjamin/Cummings, 1990.
- Beckett, B. *Introduction to Cryptology*. Malden, Massachusetts: Blackwell Scientific, 1988.
- Beckwith, Charlie A., and Donald Knox. *Delta Force*. San Diego: Harcourt Brace Jovanovich, 1983.
- Beers, M. H., and R. Berkow, eds. *The Merck Manual of Diagnosis and Therapy*. Whitehouse Station, New Jersey: Merck & Co., Inc., 2002.
- Bell, E. T. *Men of Mathematics*. Simon and Schuster, 1961.
- Bella J., Edd, and Fapta May Pt. *Amputations and Prosthetics: A Case Study Approach*. 2nd ed. New York: F. A. Davis, 2002.
- Bellairs, Angus. *The Life of Reptiles*. Vols. I and II. New York: Universe Books, 1970.
- Benenson, A.S. "Giardiasis." *Control of Communicable Diseases Manual*. Washington: American Public Health Association, 1995.
- Bennett, J.C., and Cecil F. Plum. *Textbook of Medicine*. Philadelphia: W. B. Saunders Co., 1996.
- Bennett, Richard M. *Espionage: An Encyclopedia of Spies and Secrets*. London: Virgin Books, 2002.

- Bennis, Warren G., and Patricia Ward Biederman. *Organizing Genius: The Secrets of Creative Collaboration*. Reading, MA: Addison-Wesley, 1997.
- Bennish, M.L., and C. Seas. *Current Diagnosis*, vol. 9 Philadelphia: W.B. Saunders Company, 1997.
- Benson, Robert Louis. *A History of U.S. Communications Intelligence during World War II: Policy and Administration*. Washington, D.C.: Center for Cryptologic History, National Security Agency, 1997.
- Bentley, Tom, and Jon Hastings. *Safe Computing: How to Protect Your Computer, Your Body, Your Data, Your Money and Your Privacy in the Information Age*. Concord, CA: Untechnical Press, 2000.
- Berkowitz, Bruce D., and Allan E. Goodman. *Strategic Intelligence for American National Security*. Princeton, NJ: Princeton University Press, 1989.
- Berlin, R. E. and C. C. Stanton. *Radioactive Waste Management*. New York: John Wiley & Sons, 1989.
- Berne, R. M., and M. N. Levy. *Cardiovascular Physiology*. St. Louis: C. V. Mosby, 1992.
- Bernier, Donald R., Paul E. Christian, and James K. Langan, eds. *Nuclear Medicine: Technology and Techniques*. 3rd Edition. St. Louis: Mosby, 1994.
- Beschloss, Michael R. *Mayday: Eisenhower, Khrushchev and the U-2 Affair*. New York: Harper & Row, 1986.
- Best, Richard A. *Project Echelon: U.S. Electronic Surveillance Efforts*. Washington, D.C.: Congressional Research Service, 2000.
- Best, Richard A. *The National Security Council: An Organizational Assessment*. Huntington, NY: Novinka Books, 2001.
- Best, Richard A., Jr. *Intelligence and Law Enforcement: Countering Transnational Threats to the U.S.* Washington, D.C.: Congressional Research Service, 2001.
- Bettelheim, Frederick A., and Jerry March. *Introduction to General, Organic, and Biological Chemistry*. 3rd ed. Fort Worth: Saunders College Publishing, 1991.
- Beurton, Peter, Raphael Falk, Hans-Jörg Rheinberger., eds. *The Concept of the Gene in Development and Evolution*. Cambridge, UK: Cambridge University Press, 2000.
- Bildstein, Keith L. *White Ibis: Wetland Wanderer*. Washington, D.C.: Smithsonian Institution Press, 1993.
- Binns, Tristan Boyer. *The Environmental Protection Agency* Woburn, MA: Heineman Publishers, 2002.
- Birdwell, Michael E. *Celluloid Soldiers: The Warner Bros. Campaign Against Nazism*. New York: New York University Press, 1999.
- Birkhoff, Garrett, and Saunders MacLane. *A Survey of Modern Algebra*. New York: Macmillan Co., 1947.
- Birkhoff, George David, and Ralph Beatley. *Basic Geometry*. New York: Chelsea Publishing Co., 1959.
- Birren, Bruce W., and Eric Hon Cheong Lai. *Pulsed Field Electrophoresis: A Practical Guide*. San Diego: Academic Press, 1997.
- Bishop, Chris, ed. *The Encyclopedia of Modern Military Weapons: The Comprehensive Guide to over 1,000 Weapon Systems from 1945 to the Present Day*. New York: Barnes & Noble, 1999.
- Bishop, Matt. *Computer Security: Art and Science*. Boston: Addison Wesley Professional, 2002.
- Bittar, F. Edward, ed. *Chemistry of the Living Cell*. Greenwich, CT: JAI Press, 1992.
- Bittinger, Marvin L, and Davic Ellenbogen. *Intermediate Algebra: Concepts and Applications*. 6th ed. Reading, MA: Addison-Wesley Publishing, 2001.
- Bixler, Margaret T. *Winds of Freedom: The Story of the Navajo Code Talkers of World War II*. Darien, CT: Two Bytes Publishing Company, 1992.
- Black, Ian and Benny Morris. *Israel's Secret Wars: A History of Israel's Intelligence Services*. New York: Grove Press, 1992.
- Blackstock, Paul W., and Frank L. Schaf, Jr., eds. *Intelligence, Espionage, Counterespionage, and Covert Operations: A Guide to Information Sources*. Detroit, MI: Gale Research Company, 1978.
- Blair, Clay. *The Forgotten War: America in Korea, 1950–1953*. New York: Times Books, 1987.
- Blake, Bernard, ed. *Jane's Radar and Electronic Warfare Systems*. Alexandria, VA: Jane's Information Group Inc., 1992.
- Bland W., and D. Rolls. *Weathering, an Introduction to Scientific Principles*. New York: Oxford University Press, 1988.
- Blight J.G., and D.A. Welch. *Intelligence and the Cuban Missile Crisis*. London; Portland, OR: Frank Cass, 1998.
- Blight, James, and Peter Kornbluh. *Politics of Illusion: The Bay of Pigs Invasion Reexamined*. Boulder, CO: Lynne Rienner Publishers, 1998.
- Bloomfield, Louis A. *How Things Work: The Physics of Everyday Life*. 2nd ed. New York: John Wiley & Sons, 2000.
- Bloss, F. D. *Crystallography and Crystal Chemistry*. New York: Holt, Rinehart and Winston, Inc., 1971.
- Blum, Howard. *I Pledge Allegiance*. New York: Simon and Schuster, 1987.
- Blunden, Bob. *The Money Launderers: How They Do It, and How to Catch Them at It*. Chalford, England: Management Books, 2001.
- Blyth, Andrew and Gerald L. Kovacich. *Information Assurance: Surviving in the Information Environment*. London: Springer, 2001.
- Bock, G., G. Cardew, and H. Paretzhe, eds. *Health Impacts of Large Releases of Radionuclides*. John Wiley and Sons, 1997.
- Bockris, John O'M., and Amulya K. N. Reddy. *Modern Electrochemistry*. New York: Plenum Press, 1973.
- Bodziak J., and Jon J. Nordby. *Forensic Science: An Introduction to Scientific and Investigative Techniques*. CRC Press, 2002.
- Boehm, Roy, and Charles W. Sasser. *First SEAL*. New York: Pocket Books, 1997.
- Boggs., Sam, Jr. *Principles of Sedimentology and Stratigraphy*, 2nd edition. Englewood Cliffs, NJ: Prentice Hall, 1995.
- Bohr, Niels. *The Unity of Knowledge*. New York: Doubleday & Co., 1955.
- Bohrer, David. *America's Special Forces*. St. Paul, MN: MBI Publishing, 2002.
- Boikess, Robert S., and Edward Edelson. *Chemical Principles*. 2nd edition. New York: Harper & Row Publishers, 1981.

- Bolemon, Jay. *Physics: A Window On Our World*, 3rd ed. Needham, MA: Prentice-Hall, 1995.
- Bolin, Robert L. *Technical Intelligence Bibliography*. Athens, GA: University of Georgia, Political Science Department, 1985.
- Boll, Michael M. *National Security Planning Roosevelt through Reagan*. Lexington: University Press of Kentucky, 1988.
- Bolz, Frank, et al. *The Counterterrorism Handbook: Tactics, Procedures, and Techniques*. Boca Raton, FL: CRC Press, 2002.
- Bonds, Ray, ed. *The Modern U.S. War Machine: An Encyclopedia of American Military Equipment and Strategy*. New York: Military Press, 1987.
- Borse, Henry A., Lloyd Motz, and Jefferson Hane Weaver. *The Atomic Scientists: A Biographical History*. New York: John Wiley & Sons, Inc., 1989.
- Bord, Donald J. and Vern J. Ostdiek. *Inquiry Into Physics*. 3rd ed. West Publishing Company, 1995.
- Born, Max, and Emil Wolf. *Principles of Optics*. New York: Pergamon Press, 1980.
- Borosage, Robert, and John D. Marks. *The CIA File*. New York: Grossman, 1976.
- Borth, Christy. *Mankind on the Move: The Story of Highways*. Automotive Safety Federation, 1969.
- Bosiljevac, T. J. *SEALs: UDT/SEAL Operations in Vietnam*. New York: Ivy Books, 1991.
- Boss, Martha J., Dennis W. Day, and Roger F. Jones. *Biological Risk Engineering Handbook: Infection Control and Decontamination*. Boca Raton: Lewis Publishers, Inc., 2002.
- Bossler, John D., John R. Jensen, Chris McMaster, and Chris Rizos, (eds). *Manual of Geospatial Science and Technology*. Mount Laurel, New Jersey: Taylor & Francis, 2001.
- Bosworth, Seymour (ed.), and Michel E. Kabay. *Computer Security Handbook*. New York: John Wiley & Sons, 2002.
- Bourret, Jean Claude. *GIGN, Vingt Ans D'Actions: 1974-1994*. Paris: M. Lafon, 1995.
- Bouvier, Virginia Marie. *Whose America? The War of 1898 and the Battles to Define the Nation*. Westport, CT: Praeger, 2001.
- Bowditch, W., and K. Bowditch. *Welding Technology Fundamentals*. South Holland, IL: Goodheart-Willcox, 1992.
- Boyd, Richard H., and Paul J. Phillips. *The Science of Polymer Molecules*. Cambridge University Press, 1996.
- Boyd, T. J. M., and J. J. Anderson. *The Physics of Plasma*. Cambridge, UK: Cambridge University Press, 2003.
- Boyer, Carl B. *A History of Mathematics*. 2nd ed. Revised by Uta C. Merzbach. New York: John Wiley and Sons, 1991.
- Boyle, Robert. *Gold History and Genesis of Deposits*. New York: Van Nostrand Reinhold, 1987.
- Boylstad, Robert, and Louis Nashalsky. *Electronics: A Survey*. Englewood Cliffs, NJ: Prentice Hall, 1985.
- Boyne, Walter J. *Beyond the Wild Blue: A History of the United States Air Force, 1947-1997*. New York: St. Martin's Press, 1997.
- Boyne, Walter J. *Boeing B-52: A Documentary History*. New York: Jane's, 1982.
- Brady, G. S., and H. R. Clause. *Materials Handbook*. New York: McGraw Hill, Inc, 1991.
- Brady, James E. and John R. Holum. *Fundamentals of Chemistry*. New York: Wiley, 1988.
- Brady, Russell, and John R. Holum. *Chemistry, Matter and Its Changes*. 3rd ed. New York: John Wiley and Sons Inc., 2000.
- Bramwell, Martyn. *Weather*. New York: Franklin Watts, 1994.
- Branden, C., and J. Tooze. *Introduction to Protein Structure*. New York: Garland, 1991.
- Brandrup, J., and E. H. Immergut, eds. *Polymer Handbook*. 3rd Edition. New York, NY: Wiley-Interscience, 1990.
- Branscomb, Anne W. *Who Owns Information? From Privacy to Public Access*. New York: Basic Books, 1994.
- Breckenridge, Robert P. *Modern Camouflage, the New Science of Protective Concealment*. New York: Farrar & Rinehart, 1942.
- Breckinridge, Scott D. *The CIA and the U.S. Intelligence System*. Boulder, CO: Westview Press, 1986.
- Bresler, Fenton. *Interpol*. London: Sinclair-Stevenson, 1992.
- Briggs, S.A. *Basic Guide to Pesticides. Their Characteristics and Hazards*. Washington, D.C.: Taylor & Francis, 1992.
- Brill, A. B., et al. *Low-level Radiation Effects: A Fact Book*. New York: The Society of Nuclear Medicine, 1985.
- Brock, William H. *The Norton History of Chemistry*. New York: W. W. Norton & Company, 1993.
- Brockris, J. O'M. *Energy Options*. Redfern NSW, Australia: Halsted Press, 1980.
- Brodie, Bernard and Fawn M. Brodie. *From Crossbow to H-Bomb: The Evolution of the Weapons and Tactics of Warfare*. Bloomington, IN: Indiana University Press, 1973.
- Brombacher, W. G. *Mercury Barometers and Manometers*. Washington, D.C.: U.S. Department of Commerce, National Bureau of Standards, 1960.
- Brooker, R. *Genetics Analysis and Principals*. Menlo Park: Benjamin Cummings, 1999.
- Brooks, J. *Telephone: The First Hundred Years*. Harper & Row, 1976.
- Browder, George C. *Hitler's Enforcers: The Gestapo and SS Security Service in the Nazi Revolution*. Oxford: Oxford University Press, 1996
- Brown, Anthony Cave. *The Last Hero: Wild Bill Donovan*. New York: Times Books, 1982.
- Brown, Harold, and Franklin Neva. *Basic Clinical Parasitology*. Norwalk, CT: Appleton-Century-Crofts, 1983.
- Brown, Julian. *Minds, Machines, and the Multiverse: The Quest for the Quantum Computer*. New York: Simon & Schuster, 2000.
- Brown, William H., and Elizabeth Rogers. *General, Organic and Biochemistry*. Boston: Willard Grant, 1980.
- Browne, J. P. R. *Electronic Warfare*. London: Brassey's, 1998.
- Brugioni, Dino A. *Eyeball to Eyeball: The Inside Story of the Cuban Missile Crisis*. New York: Random House, 1990.
- Brugioni, Dino A. *From Balloons to Blackbirds: Reconnaissance, Surveillance and Imagery Intelligence: How It Evolved*. McLean, VA: Association of Former Intelligence Officers, 1993.
- Brugioni, Dino A. *Photo Fakery: The History and Techniques of Photographic Deception*. Washington, D.C.: Brassey's, 1999.

- Bruice, Paula. *Organic Chemistry*. 3rd ed. Englewood Cliffs, NJ: Prentice-Hall, 2001.
- Buchanan, B. B., W. Gruissem, and R. L. Jones. *Biochemistry and Molecular Biology of Plants*. Rockville, MD: American Society of Plant Physiologists, 2000.
- Buchanan, R.E., and N.E. Gibbons. *Bergey's Manual of Determinative Bacteriology*, 8th ed. Baltimore: The Williams & Wilkins Company, 1974.
- Buck, Alice L. *A History of the Atomic Energy Commission*. U.S. Department of Energy, 1983.
- Budavari, Susan, editor. *The Merck Index*. Merck Research Laboratories, 1996.
- Budiansky, Stephen. *Battle of Wits: The Complete Story of Codebreaking in World War II*. New York: Touchstone Books, 2002.
- Buechel, K.H., et al. *Industrial Inorganic Chemistry*. New York: VCH, 2000.
- Buelow, George, and Suzanne Hebert. *Counselor's Resource on Psychiatric Medications, Issues of Treatment and Referral*. Pacific Grove, CA: Brooks/Cole, 1995.
- Buranelli, Vincent, and Nan Buranelli. *Spy Counterspy: An Encyclopedia of Espionage*. New York: McGraw-Hill, 1982.
- Bureau of Alcohol, Tobacco, and Firearms: Its History, Progress, and Programs*. Washington, D.C.: U.S. Government 1995.
- Burn R. P. *A Pathway Into Number Theory*. 2nd. ed. New York: Cambridge University Press, 1997.
- Burnham, David. *A Law unto Itself: Power, Politics, and the IRS*. New York: Random House, 1989.
- Burrough, P.A. and R.A. McDonnell. *Principles of Geographic Information Systems*, 2nd ed. Oxford: University Press, 1998.
- Burrows, William E. *By Any Means Necessary: America's Secret Air War in the Cold War*. New York: Farrar, Straus and Giroux, 2001.
- Burrows, William. *Deep Black: Space Espionage and National Security*. New York: Random House, 1986.
- Burton, David M. *The History of Mathematics*, 5th Ed. New York: McGraw Hill College Division, 2002.
- Busby, Robert. *Reagan and the Iran-Contra Affair*. Chippenham, Wiltshire, Great Britain: Macmillan, 1999.
- Bushart, Howard L. *Soldiers of God: White Supremacists and Their Holy War for America*. New York: Kensington, 1998.
- Butler, Richard. *The Greatest Threat: Iraq, Weapons of Mass Destruction, and the Crisis of Global Security*. New York: Public Affairs, 2001.
- Bynum, W. F., E. J. Browne, and Roy Porter. *Dictionary of the History of Science*. Princeton, NJ: Princeton University Press, 1981.
- Cabinet Office. *National Intelligence Machinery*. London: HMSO, 2000.
- Cahill, M. *Handbook of Diagnostic Tests*. Springhouse Company, 1995.
- Cairns, J., G. S. Stent, and J. D. Watson, eds. *Phage and the Origins of Molecular Biology*, 2nd ed. New York: Cold Spring Harbor Laboratory of Quantitative Biology, 1992.
- Calder, James, comp. *Intelligence, Espionage and Related Topics: An Annotated Bibliography of Serial Journal and Magazine Scholarship, 1844–1998*. Westport, CT: Greenwood, 1999.
- Calhoun, Frederick S. *The Trainers: The Federal Law Enforcement Training Center and the Professionalization of Federal Law Enforcement*. Washington, D.C.: U.S. Government Printing Office, 1996.
- Cameron, Gavin. *Nuclear Terrorism: A Threat Assessment for the 21st Century*. New York: St. Martin's Press, 1999.
- Campbell, A. M. "Monoclonal Antibodies." In *Immunochemistry*, edited by Carol J. van Oss and Marc H. V. van Regenmortel. New York: Marcel Dekker, Inc., 1994.
- Campbell G.L., and D.T. Dennis. "Plague and other Yersinia Infections." In: Kasper DL, et al; eds. *Harrison's Principles of Internal Medicine*, 14th ed. New York: McGraw Hill, 1998.
- Campbell, James B. *Introduction to Remote Sensing (3rd edition)*. New York: Guilford Press, 2002.
- Campbell, Kurt M., and Michele A. Flournoy. *To Prevail: An American Strategy for the Campaign Against Terrorism*. Washington, D.C.: CSIS Press, 2001.
- Campbell, N., J. Reece, and L. Mitchell. *Biology*. 5th ed. Menlo Park: Benjamin Cummings, Inc., 2000.
- Cannon, Don L. *Understanding Solid-State Electronics*. 5th ed. SAMS division of Prentice Hall Pub. Co., 1991.
- Canton, Bruce. *The Civil War*. American Heritage/Wings Books, New York/Avenel, NJ, 1960.
- Cantor, Norman F. *In the Wake of the Plague: The Black Death and the World It Made*. New York: Perennial, 2002.
- Cantwell, John D. *The Second World War: A Guide to Documents in the Public Record Office*. London: PRO, 1998.
- Caplan, Arthur L., ed. *When Medicine Went Mad: Bioethics and the Holocaust*. Totowa, N.J.: Humana, 1992.
- Carey, Francis A., and Richard J. Sundberg. *Advanced Organic Chemistry: Structure and Mechanisms*. 4th ed. New York: Plenum, 2001.
- Carey, Joseph, ed. *Brain Facts, A Primer on the Brain and the Nervous System*. Washington, D.C.: Society for Neuroscience, 1993.
- Carl, Leo D. *The CIA Insider's Dictionary of U.S. and Foreign Intelligence, Counterintelligence, and Tradecraft*. Washington, D.C.: NIBC Press, 1996.
- Carlisle, Rodney P. *Encyclopedia of the Atomic Age*. New York: Facts on File, 2001.
- Carlisle, Rodney P., with Joan M. Zenzen. *Supplying the Nuclear Arsenal: American Production Reactors, 1942–1992*. Baltimore: John Hopkins University Press, 1996.
- Carney, John T., and Benjamin F. Schemmer. *No Room for Error: The Covert Operations of America's Special Tactics Units from Iran to Afghanistan*. New York: Ballantine, 2002.
- Caro, Paul. *Water*. New York: McGraw Hill, 1993.
- Carroll, Felix A. *Perspectives on Structure and Mechanism in Organic Chemistry*. Pacific Grove, CA: Brooks/Cole Publishing Company, 1998.
- Carroll, Peter N. *It Seemed Like Nothing Happened: America in the 1970s*. New Brunswick: Rutgers University Press, 1990.

- Carter, Richard. *Breakthrough: The Saga of Jonas Salk*. Naples, FL: Trident Press, 1966.
- Cassaro, Edward, and Linda Lomonaco. *Operators Guide: Atmospheric Release Advisory Capability (ARAC) Site Facility*. Springfield, VA: Department of Energy, 1979.
- Causewell, Erin V. *National Missile Defense: Issues and Developments*. New York: Novinka Books, 2002.
- Cefrey, Holly, et al. *Epidemics: Deadly Diseases Throughout History (The Plague, AIDS, Tuberculosis, Cholera, Small Pox, Polio, Influenza, and Malaria)*. New York: Rosen Publishing Group, 2001.
- Chalker, Dennis C., and Kevin Dockery. *One Perfect Op: An Insider's Account of the Navy SEAL Special Warfare Teams*. New York: Morrow, 2002.
- Chalou, George C. *Scientific and Technical Intelligence Gathering*. New York: Garland Publishing, 1989.
- Chalou, George C. *The Secrets of War: The Office of Strategic Services in World War II*. Washington, D.C.: National Archives and Records Administration, 1992.
- Chandrasekhar, S. *Liquid Crystals*. 2nd ed. Cambridge University Press, 1992.
- Chang, Laurence, ed. *Cuban Missile Crisis, 1962: A National Security Archive Documents Reader (National Security Archive Documents Reader)*. Washington, D.C.: United States Government Press, 1998.
- Chang, Raymond. *Chemistry*. New York: McGraw-Hill, 1991.
- Chant, Christopher. *The Encyclopedia of Codenames of World War II*. London: Routledge & Kegan Paul, 1986.
- Chant, Christopher. *An Illustrated Data Guide to Modern Reconnaissance Aircraft*. London: Tiger Books International, 1997.
- Chapman, Robert, et al. *COPS Innovations: A Closer Look: Local Law Enforcement Responds to Terrorism: Lessons in Prevention and Preparedness*. Washington, D.C.: U.S. Department of Justice Office of Community Oriented Policing Services.
- Charthouse, Robert. *Codes and Ciphers*. Cambridge, England: Cambridge University Press, 2002.
- Chen, C. H. *Information Processing for Remote Sensing*. River Edge, NJ: World Scientific, 1999.
- Cheswick, William R., Steven M. Bellovin, and Aviel D. Rubin. *Firewalls and Internet Security: Repelling the Wiley Attacker*, 2nd edition. Boston: Addison Wesley Professional, 2003.
- Cheung, Kin P. *Plasma Charging Damage*. Berlin: Springer Verlag, 2000.
- Chikazumi, S. *Physics of Magnetism*. New York: John Wiley & Sons, Ltd., 1984.
- Child, Graham. *Sound*. Garden City, NY: Doubleday Science Series, Doubleday and Company, Inc., 1970.
- Chin, J. "Tularemia." In *Control of Communicable Diseases Manual*. Washington, D.C.: American Public Health Association, 2000.
- Chranowski, Edward J. *Active Radar Electronic Countermeasures*. Norwood, MA: Artech House, 1990.
- CIA History Staff. *CIA Cold War Records: CORONA—America's First Satellite Program*. Washington, D.C., 1995.
- CIA History Staff. *CIA Cold War Records: The CIA Under Harry Truman*. Washington, D.C.: CIA, 1994.
- Cimbala, Stephen J. *Nuclear Strategy in the Twenty-First Century*. Westport, CT: Praeger, 2000.
- Cirincione, Joseph, Jon B. Wolfsthal, Miriam Rajkuman, and Jessica T. Mathews. *Deadly Arsenals: Tracking Weapons of Mass Destruction*. Washington, D.C.: Carnegie Endowment for International Peace, 2002.
- Clancy, Tom. *Carrier: A Guided Tour of an Aircraft Carrier*. New York: Berkley Books, 1999.
- Clancy, Tom. *Fighter Wing: A Guided Tour of an Air Force Combat Wing*. New York: Berkley Books, 1995.
- Clark, Wesley K. *Waging Modern War: Bosnia, Kosovo, and the Future of Combat*. New York: Public Affairs, 2001.
- Clarke, C. A. *Human Genetics and Medicine*, 3rd ed. Baltimore, MD: E. Arnold, 1987.
- Cleroux, Richard. *Official Secrets: The Story Behind the Canadian Security Intelligence Service*. Toronto: McGraw-Hill Ryerson, 1990.
- Closing the Circle on the Splitting of the Atom: The Environmental Legacy of Nuclear Weapons Production in the United States and What the Department of Energy Is Doing About It*. Washington, D.C.: U.S. Government Printing Office, 1995.
- Clydesdale, Fergus, ed. *Food Science and Nutrition: Current Issues and Answers*. Englewood Cliffs, N.J.: Prentice-Hall, 1979.
- Cobb, Cathy, and Harold Goldwhite. *Creations of Fire: Chemistry's Lively History from Alchemy to the Atomic Age*. New York: Plenum Press, 1995.
- Cochran, Thomas B., William M. Arkin, and Milton M. Hoenig. *Nuclear Weapons Databook: Vol. 1, U.S. Nuclear Forces and Capabilities*. Cambridge, MA: Ballinger Publishing Company, 1984.
- Coggins, Jack. *Arms and Equipment of the Civil War*. Wilmington, NC: Broadfoot Publishing Company, 1990.
- Cohen, Susan, and Daniel Cohen. *Pan Am 103: The Bombing, the Betrayals, and the Bereaved Families' Search for Justice*. New York: Signet, 2001.
- Cohn, Victor. *News and Numbers. A Guide to Reporting Statistical Claims and Controversies in Health and Related Fields*. Ames: Iowa State University Press, 1989.
- Colby, William E. *Honorable Men—My Life in the CIA*. New York: Simon and Schuster, 1978.
- Colby, William E., with James McCarger. *Lost Victory: A Firsthand Account of America's Sixteen-Year Involvement in Vietnam*. Chicago: Contemporary Books, 1989.
- Cole, Leonard A. *The Eleventh Plague: The Politics of Biological and Chemical Warfare*. New York: WH Freeman and Company, 1996.
- Colliers, A., et al. *Microbiology and Microbiological Infections*, vol. 3. London: Edward Arnold Press, 1998.
- Collin, Richard H. *Theodore Roosevelt's Caribbean: The Panama Canal, the Monroe Doctrine, and the Latin American Context*. Baton Rouge: Louisiana State University Press, 1990.
- Collings, Peter J. *Liquid Crystals: Nature's Delicate Phase of Matter*. Princeton University Press, 1990.



- Collins, A. Frederick. "Vacuum Tubes." *The Radio Amateur's Handbook*. revised by Robert Herzberg. New York: Harper & Row, 1983.
- Collins, A. G., and A. I. Johnson, eds. *Ground-Water Contamination: Field Methods*. Philadelphia: American Society for Testing and Materials, 1988.
- Collins, Mark, ed. *The Last Rain Forests*. London: Mitchell Beazley Publishers, 1990.
- Combatting Terrorism: How Five Foreign Countries Are Organized to Combat Terrorism*. Washington, D.C.: General Accounting Office, 2000.
- Comer, Ronald J. *Abnormal Psychology*. 2nd ed. New York: W. H. Freeman, 2000.
- Communications Management and Control Activity (CMCA)*. Washington, D.C.: Defense Information Systems Agency, 1995.
- Conboy, Kenneth J. *Feet to the Fire: CIA Covert Operations in Indonesia*. Annapolis MD: Naval Institute Press, 1999.
- Conboy, Kenneth J., and Dale Andradé. *Spies and Commandos: How America Lost the Secret War in North Vietnam*. Lawrence, KS: University Press of Kansas, 2000.
- Conboy Kenneth J., and J. Morrison. *The CIA's Secret War in Tibet*. Lawrence, KS: University Press of Kansas, 2002.
- Congressional Research Service. *The United States Intelligence Community: A Brief Description of Organization and Functions*. Washington, D.C.: Library of Congress, 1975.
- Connors, Edward F. *Convicted by Juries, Exonerated by Science: Case Studies in the Use of DNA Evidence to Establish Innocence After Trial*. Washington, D.C.: National Institute of Justice, 1996.
- Conroy, John. *Unspeakable Acts: The Dynamics of Torture*. New York: Alfred A. Knopf, 2000.
- Constantinides, George C. *Intelligence and Espionage: An Analytical Bibliography*. Boulder, CO.: Westview Press, 1983.
- Cook, Don. *Forging the Alliance: The Birth of the NATO Treaty and the Dramatic Transformation of U.S. Foreign Policy Between 1945 and 1950*. New York: Arbor House/William Morrow, 1989.
- Cord Meyer. *Facing Reality: From World Federalism to the CIA*. New York: Harper & Row, 1980.
- Cordesman, Anthony H. *Terrorism, Asymmetric Warfare, and Weapons of Mass Destruction: Defending the U.S. Homeland*. Westport, CT: Praeger, 2002.
- Cordesman, Anthony H., and Justin G. Cordesman. *Cyber-Threats, Information Warfare, and Critical Infrastructure Protection: Defending the U.S. Homeland*. Westport, CT: Praeger, 2002.
- Cormican, M. G. and M. A. Pfaller. "Molecular Pathology of Infectious Diseases." *Clinical Diagnosis and Management by Laboratory Methods*. 20th ed. Philadelphia: W. B. Saunders, 2001.
- Corvo, Max. *The O.S.S. in Italy, 1942-1945: A Personal Memoir*. New York: Praeger, 1990.
- Cotran, Ramzi S., et al. *Robbins Pathologic Basis of Disease*. Philadelphia: W. B. Saunders Company, 1994.
- Coughlan, G. D. and J. E. Dodd. *The Ideas of Particle Physics*. 2nd ed. Cambridge: Cambridge University Press, 1991.
- Courant, Richard, and Herbert Robbins. *What Is Mathematics?* Oxford: Oxford University Press, 1948.
- Couzens, E. G. and V. E. Yarsley. *Plastics in the Modern World*. Baltimore, MD: Penguin, 1968.
- Cowan, Henry J. *The Master Builders*. New York: Wiley, 1977.
- Crabb, Cecil V. and Kevin V. Mulcahy. *American National Security: A Presidential Perspective*. Pacific Grove, CA: Brooks/Cole, 1991.
- Craft, B.C. *Applied Petroleum Reservoir Engineering*, 2nd Edition. Englewood Cliffs, NJ: Prentice Hall, Inc., 1991.
- Craig, Gordon Alexander, and Francis J. Lowenheim. *The Diplomats, 1939-1979*. Princeton, NJ: Princeton University Press, 1994.
- Craig, James, David Vaughan, and Brian Skinner. *Resources of the Earth*. Englewood Cliffs, New Jersey: Prentice Hall, 1988.
- CRC Handbook of Chemistry and Physics*. Boston: CRC Press, Inc., published yearly.
- Crickmore, Paul F. *Lockheed SR-71: The Secret Missions Exposed*. London: Osprey, 1988.
- Critical Foundations: Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection*. Washington, D.C.: The Commission, 1997.
- Croall, C., and S. Sempler. *Nuclear Power for Beginners*. New York: State Mutual Books, 1990.
- Cross, Wilbur. *Petroleum*. Chicago: Children's Press, 1983.
- Cumpsty, Nicholas A. *Jet Propulsion: A Simple Guide to the Aerodynamic and Thermodynamic Design and Performance of Jet Engines*. Cambridge: Cambridge University Press, 1998.
- Curtis, A. R. *Space Almanac*. Arcsoft Publishers, 1990.
- Cutnell, John D., and Kenneth W. Johnson. *Physics*. 3rd ed. New York: Wiley, 1995.
- Dahl, Per F. *Heavy Water and the Wartime Race for Nuclear Energy*. Bath, UK: Institute of Physics Publishing, 1999.
- Daintith, John and D. Gjertsen, eds. *A Dictionary of Scientists*. New York: Oxford University Press, 1999.
- Dallas, Gregor. *The Final Act: the Roads to Waterloo*. New York: Henry Holt and Co., 2001.
- Dalton, Patricia A. *Combating Terrorism: Enhancing Partnerships through a National Preparedness Strategy*. Washington, D.C.: General Accounting Office, 2002.
- Danaher, Kevin, editor. *Fifty Years is Enough: The Case Against the World Bank and the International Monetary Fund*. Cambridge, MA: South End Press, 1994.
- Danby, J. M. A. *Computer Modeling: From Sports to Spaceflight—From Order to Chaos*. Richmond, VA: Willmann-Bell, 1997.
- Dando, Malcolm. *Biological Warfare in the 21st Century*. New York: Macmillan, 1994.
- Danielson, Eric W., James Levin, and Elliot Abrams. *Meteorology*. 2nd ed. with CD-ROM. Columbus: McGraw-Hill Science/Engineering/Math, 2002.
- Dantzig, Tobias. *Number, the Language of Science*. Garden City, NY: Doubleday and Co., 1954.
- Darby, N. J., and T. E. Creighton. *Protein Structure*. New York: Oxford University Press, 1994.
- Darling, Arthur. *The Central Intelligence Agency An Instrument of Government to 1950*. State College: Pennsylvania State University Press, 1990.

- Darnell, J., H. Lodish, and D. Baltimore. *Molecular Cell Biology*. New York: Scientific American Books, Inc., 1986.
- Das, Ashok and Thomas Ferbel. *Introduction to Nuclear and Particle Physics*. John Wiley, 1994.
- Daughtery, William J. *In the Shadow of the Ayatollah: A CIA Hostage in Iran*. Annapolis, MD: Naval Institute Press, 2001.
- Davenport, Harold. *The Higher Arithmetic: An Introduction to the Theory of Numbers*. 6th edition. Cambridge: Cambridge University Press, 1992.
- Davidovits, Peter. *Communication*. New York: Holt, Rinehart and Winston, Inc., 1972.
- Davies, Philip H. J. *The British Secret Services*. Brunswick, NJ: Transaction Publishers, Rutgers University, 1996.
- Davis, Brian L. *Qaddafi, Terrorism, and the Origins of the U.S. Attack on Libya*. New York: Praeger, 1990.
- Davis, Charles O. *Across the Mekong: The True Story of an Air America Helicopter Pilot*. Hildesheim Press, 2000.
- Davis, James Kirkpatrick. *Spying on America: The FBI's Domestic Counterintelligence Program*. New York: Praeger, 1992.
- Davis, Joel. *Mapping the Code: The Human Genome Project and the Choices of Modern Science*. Wiley, 1990.
- Davis, Richard A., Jr. *Oceanography, An Introduction to the Marine Environment*. Dubuque, IA: William C. Brown Publishers, 1991.
- Davis, S. N., and R. J. M. DeWiest. *Hydrogeology*. New York: Wiley, 1966.
- Davis, Shelley L. *Unbridled Power: Inside the Secret Culture of the IRS*. New York: HarperBusiness, 1997.
- Day, Dwayne A., and John M. Logsdon. *Eye in the Sky: The Story of the Corona Spy Satellites*. Washington, D.C.: Smithsonian Institution Press, 1998.
- De Bono, Edward. *Eureka! An Illustrated History of Inventions From the Wheel to the Computer*. London: Thames and Hudson, 1974.
- De Gennes, P.G., and J. Prost. *The Physics of Liquid Crystals*. 2nd ed. Oxford Science Publications, 1993.
- De Riaz, Yvan A. *The Book of Knives*. New York: Crown, 1981.
- Dean, John A., ed. *Lange's Handbook of Chemistry*. 15th ed. New York: McGraw-Hill, 199.
- Deavours, Cipher, et al. *Cryptology: Machines, History & Methods*. Norwood, MA: Artech House, 1989.
- The Defense Information Systems Agency (DISA): NAA, "The Three Sisters."* Washington, D.C.: Defense Information Systems Agency, 1995.
- Dehqanzada, Yahya A., and Ann Florini. *Secrets for Sale: How Commercial Satellite Imagery Will Change the World*. Washington, D.C.: Carnegie Endowment for International Peace, 2000.
- Del Bimbo, Alberto. *Visual Information Retrieval*. San Francisco: Morgan Kaufmann Publishers, 1999.
- Delaney, C. F. G., and E. C. Finch. *Radiation Detectors*. New York: Oxford University Press, 1992.
- Delaporte, François. *Disease and Civilization: The Cholera in Paris, 1832*. Cambridge: MIT Press, 1986.
- The Department of Justice Manual*. Gaithersburg, MD: Aspen Law & Business, 2000.
- Department of the Treasury. *Excerpts from the History of the United States Secret Service, 1865–1875*. Washington, D.C.: Department of the Treasury, 1978.
- Deriabin J.L., and P. Deriabin. *The Spy Who Saved the World: How a Soviet Colonel Changed the Course of the Cold War*. New York: Scribner's, 1992.
- Dessler, A. *The Chemistry and Physics of Stratospheric Ozone*. Cornwall, UK: Academic Press, 2000.
- Devore, Ronald M. *Spies and All That: Intelligence Agencies and Operations; A Bibliography*. Los Angeles: California State University, Center for the Study of Armament and Disarmament, 1977.
- DeVorkin, D. H. *Race to the Stratosphere*. Springer-Verlag, 1989.
- Diagnostic and Statistical Manual of Mental Disorders, DSM-IV*. Washington, DC: American Psychiatric Association, 1994.
- Dickson, Leonard Eugene. *History of the Theory of Numbers*. Providence, RI: American Mathematical Society, 1999.
- Dickson, T.R. *Introduction to Chemistry*. Wiley and Sons, 1991.
- Diffie, Whitfield, and Susan Eva Landau. *Privacy on the Line: The Politics of Wiretapping and Encryption*. Cambridge, MA: MIT Press, 1998.
- D'Ignazio, Fred. *Working Robots*. New York: Elsevier/Nelson Books, 1982.
- Disclosure of Classified Information to Congress*. Washington, D.C.: U.S. Government Printing Office, 1998.
- Disposition of Production Records of the Defense Intelligence Agency: A NARA Evaluation*. Washington, D.C.: National Archives and Records Administration, 1996.
- Dixon, Dougal, and Raymond L. Bernor, ed. *The Practical Geologist*. New York: Simon and Schuster, 1992.
- Dobson, C., R. Payne. *War Without End: The Terrorists, An Intelligence Dossier*. London: Harrap Limited, 1986.
- DOD Investigation Programs: Background Data*. Washington, D.C.: United States General Accounting Office 1989.
- Doerfler, Walter, and Petra Bohm, eds. *Virus Strategies: Molecular Biology and Pathogenesis*. New York: VCH, 1993.
- Doremus, R. H. *Glass Science*. New York: Wiley, 1990.
- Dorril, Stephen. *MI6: Inside the Cover World of Her Majesty's Secret Intelligence Service*. New York: Free Press, 2000.
- Dorwart, Jeffery M. *The Office of Naval Intelligence: The Birth of America's First Intelligence Agency, 1865–1918*. Annapolis, MD: Naval Institute Press, 1979.
- Doyle, M.P., and V.S. Padye. *Escherichia coli In Foodborne Bacterial Pathogens*. New York: Marcel Dekker, Inc., 1989.
- Drell, S.D. *The New Terror: Facing the Threat of Biological and Chemical Weapons*. Stanford, CA: Hoover Institute Press, 1999.
- Drell, Sidney D., Philip J. Farley, and David Holloway. *The Reagan Strategic Defense Initiative: A Technical, Political, and Arms Control Assessment*. Cambridge, MA: Ballinger Publishing Co, 1990.
- Drew, W. Lawrence. "Chlamydia." *Sherris Medical Microbiology: An Introduction to Infectious Diseases*, 3rd ed. Ed. Kenneth J. Ryan. Norwalk, CT: Appleton & Lange, 1994.

- Duffner, Robert. *Airborne Laser: Bullets of Light*. New York: Plenum Trade, 1997.
- Dulles, Allen. *The Craft of Intelligence*. New York: Harper and Row, 1963.
- Dunlop, John. *Automation and Technological Change*. Englewood Cliffs, NJ: Prentice-Hall, 1962.
- Durant, Will and Ariel. *The Age of Napoleon*. New York: Simon and Schuster, 1975.
- Dwyer, Jim. *Two Seconds under the World: Terror Comes to America*. New York: Crown Publishers, 1994.
- Dyson, Norman A. *X Rays in Atomic and Nuclear Physics*. White Plains, NY: Longman, 1973.
- Dziak, John J. *Chekisty: A History of the KGB*. Massachusetts: D. C. Heath and Company, 1988.
- Eagleman, Joe R. *Meteorology: The Atmosphere in Action*. 2nd ed. Belmont, CA: Wadsworth Publishing Company, 1985.
- Earley, Pete. *Confessions of a Spy: The Real Story of Aldrich Ames*. New York: G.P. Putnam's Sons, 1997.
- Ebbing, Darrell. *General Chemistry*. 3d ed. Boston: Houghton Mifflin, 1990.
- Ebinger, Charles K. *Nuclear Power: The Promise of New Technologies*. Washington, D.C.: CSI Studies, 1991.
- Edde, Byron. *RADAR: Principles, Technology, Applications*. Englewood Cliffs, NJ: PTR Prentice Hall, 1993.
- Edelstein, Herbert A. *Introduction to Data Mining and Knowledge Discovery, Third Edition*. Potomac, MD: Two Crows Corporation, 1999.
- Edwardes, Michael. *Playing the Great Game: A Victorian Cold War*. London: Hamish Hamilton, 1975.
- Einstein, Albert. *Relativity: The Special and General Theory*. New York: Crown, 1961.
- Eisenberg, Dennis, Uri Dan, and Eli Landau. *The Mossad Inside Stories: Israel's Secret Intelligence Service*. New York: Paddington Press, 1978.
- Eisenbud, M. *Environmental Radioactivity*. New York: Norton, 1987.
- Eisenbud, M., and T. F. Gesell. *Environmental Radioactivity: From Natural, Industrial, and Military Sources*. Academic Press, 1997.
- El-Rabbany, Ahmed. *Introduction to GPS: The Global Positioning System*. Norwood, MA: Artech Publishing, 2002.
- Ellis, Richard J. *The Dark Side of the Left: Illiberal Egalitarianism in America*. Lawrence, KS: University Press of Kansas, 1998.
- Ellis, Richard. *Encyclopedia of the Sea*. New York: Knopf, 2000.
- Ellison, D. Hank. *Handbook of Chemical and Biological Warfare Agents*. Boca Raton, FL: CRC Press, 1999.
- Elliston, Jon (introduction). *INTERRORgation: The CIA's Secret Manual on Coercive Questioning*, 2nd edition. San Francisco: AK Press, 1999.
- Ellman, Steven J., and John S. Antrobus, eds. *The Mind in Sleep: Psychology and Psychophysiology*. New York: John Wiley & Sons, 1991.
- Emerson, Steven, and Brian Duffy. *The Fall of Pan Am 103*. New York: Putnam, 1990.
- Emmer, Michele. *The Visual Mind: Art and Mathematics*. Cambridge, MA: MIT Press, 1993.
- Emsley, John. *Nature's Building Blocks: An A-Z Guide to the Elements*. Oxford: Oxford University Press, 2002.
- Emsley, John. *The Elements*. 3rd ed. New York: Oxford University Press, Inc., 1998.
- Engh, T. Abel. *Principles of Metal Refining*. New York: Oxford University Press, 1992.
- Engineered Materials Handbook*. Metals Park, OH: ASM International, 1988.
- Eoghan, Casey. *Digital Evidence and Computer Crime*. New York: Academic Press, 2000.
- EPCRA: Emergency Planning and Community Right-to-Know Act*. Chicago: American Bar Association Section of Environment, Energy, and Resources, 2002.
- Epstein, L.C. *Thinking Physics: Practical Lessons in Critical Thinking*. 2nd ed. San Francisco: Insight Press, 1994.
- Epstein, Leon D. *British Politics in the Suez Crisis*. Urbana: University of Illinois Press, 1964.
- Eras, Vincent J. M. *Locks and Keys Throughout the Ages*. Schiedam: Interbook International, 1975.
- Ernst & Young. "The Economic Contributions of the Biotechnology Industry to the U.S. Economy." *Biotechnology Industry Organization*. 2000.
- Eshed, Haggai. *Reuven Shiloah: The Man Behind the Mossad: Secret Diplomacy in the Creation of Israel*. Portland, OR: F. Cass, 1997.
- Essenfeld, Bernice, Carol R. Gontang, and Randy Moore. *Biology*. Menlo Park: Addison Wesley, 1996.
- Euclid. *Elements*. Translated by Sir Thomas L. Heath. New York: Dover Publishing Co., 1956.
- Evans A.M. *An Introduction to Economic Geology and its Environmental Impact*. Blackwell Science, 1997.
- Evans, Anthony. *Ore Geology and Industrial Minerals: An Introduction*. Boston: Blackwell Scientific Publications, 1993.
- Evans, Brian. *Understanding Digital TV: The Route to HDTV*. New York, NY: IEEE Press, 1995.
- Evans, Charles M. *The War of the Aeronauts: A History of Ballooning during the Civil War*. Mechanicsburg, PA: Stackpole Books, 2002.
- Evans, Collin. *The Casebook of Forensic Detection: How Science Solved 100 of the World's Most Baffling Crimes*. New York: Wiley, 1996.
- Evans, E.A. *Tritium and its Compounds*. New York: Wiley, Inc., 1974.
- Eves, Howard Whitley. *Foundations and Fundamental Concepts of Mathematics*. New York: Dover, 1997.
- Ewing, Alphonse B. *USA Patriot Act*. Hauppauge, N.Y.: Nova Science Publishing, 2003.
- Ewing, Galen W. *Instrumental Methods of Chemical Analysis*. 4th ed. New York: McGraw-Hill Book Company, 1975.
- Fah-Chun Cheong. *Internet Agents: Spiders, Wanderers, Brokers, and 'Bots*. Indianapolis, IN: New Riders, 1996.
- Fain, Tyrus G., and Katharine C. Plant. *The Intelligence Community: History, Organization, and Issues*. New York: R. R. Bowker, 1977.

- Fairchild, D. M. *Ground Water Quality and Agricultural Practices*. Chelsea, MI: Lewis, 1988.
- Faith, W.L., Donald Keyes, and Ronald Clark. *Industrial Chemicals*. New York: John Wiley & Sons, 1966.
- Falcoff, Mark. *Panama's Canal: What Happens When the United States Gives a Small Country What It Wants*. Washington, D.C.: AEI Press, 1998.
- Farson, Stuart, and Catherine J. Matthews. *Criminal Intelligence and Security Intelligence: A Selected Bibliography*. Toronto: Center of Criminology, University of Toronto, 1990.
- Feather, Ralph M. et al. *Science Connections*. Columbus, OH: Merrill Publishing Company, 1990.
- Feis, William B. *Grant's Secret Service: The Intelligence War from Belmont to Appomattox*. Lawrence, KS: University Press of Kansas, 2002.
- Feldman, Anthony, and Peter Ford. *Scientists & Inventors*. New York: Facts on File, 1979.
- Felix, Antonia. *Condi: The Condoleeza Rice Story*. New York: Newmarket Press, 2002.
- Felix, Christopher. *A Short Course in the Secret War*. New York: Dell Books, 1988.
- Ferbrache, David. *Germany*. Springer Verlag, 1992.
- Ferguson, Amanda, and Nancy L. Stair. *The Attack on U.S. Servicemen at Khobar Towers in Saudi Arabia on June 25, 1996*. New York: Rosen Publishing Group, 2003.
- Fermi, Rachel and Esther Samra. *Picturing the Bomb: Photographs from the Secret World of the Manhattan Project*. New York: H.N. Abrams, 1995.
- Fewsmith, Joseph. *China Since Tiananmen*. Cambridge University Press, 2001.
- Feynman, Leighton, and Sands. *The Feynman Lectures on Physics*. New York: Addison-Wesley, 1989.
- Fialka, John J. *War By Other Means: Economic Espionage in America*. New York: W. W. Norton & Company, 1997.
- Field, George, and Donald Goldsmith. *The Space Telescope*. Chicago: Contemporary Books, 1989.
- Fields, Bernard N., Peter M. Howley, and Diane E. Griffin (eds.). *Virology*. Philadelphia: Lippincott Williams & Wilkins, 2001.
- Finn, Elizabeth A. *Pox Americana: Great Smallpox Epidemic of 1775–82*. New York: Hill & Wang, 200.
- Finnegan, John Patrick, and Romana Danysh. *Military Intelligence*. Washington, D.C.: Center of Military History, United States Army, 1998.
- Finney, Thomas, Demana, and Waits. *Calculus: Graphical, Numerical, Algebraic*. Reading Mass.: Addison Wesley Publishing Co., 1994.
- Firschein, Oscar, and Thomas M. Strat. *RADIUS: Image Understanding for Imagery Intelligence*. San Francisco: Morgan Kaufmann Publishers, 1997.
- Fischer, Ben B. *At Cold War's End: U.S. Intelligence on the Soviet Union and Eastern Europe*. Washington, D.C.: Center for the Study of Intelligence, 1999.
- Fischer, Ben B. *Okhrana: The Paris Operations of the Russian Imperial Police*. Washington, D.C.: Center for the Study of Intelligence, 1997.
- Fischetti, Vincent, Richard P. Novick, Joseph J. Ferretti, and Danile A. Portnoy. *Gram-Positive Pathogens*. Washington: American Society for Microbiology Press, 2000.
- Fisher, David E. *Fire and Ice: The Greenhouse Effect, Ozone Depletion, and Nuclear Winter*. New York: Harper & Row, 1990.
- Fitch, J. Patrick. *Synthetic Aperture RADAR*. West Hanover, MA: Springer-Verlag, 2001.
- Fites, Philip, Peter Johnston, and Martin Kratz. *The Computer Virus Crisis*. New York: Van Nostrand Reinhold, 1992.
- Fitzgerald, Merni Ingrassia. *The Voice of America*. New York: Dodd, Mead, 1987.
- Fleissner, Jennifer. *The Federal Communications Commission*. New York: Chelsea House Publishers, 1992.
- Fleming, D. O., and D. L. Hunt. *Biological Safety: Principles and Practices*. 3rd ed. Washington: American Society for Microbiology, 2000.
- Fleming, D.O., and D.L. Hunt. *Biological Safety: Principles and Practices*, 3rd ed. Washington: American Society for Microbiology, 2000.
- Flint, S.J., et al. *Principles of Virology: Molecular Biology, Pathogenesis, and Control*. Washington: American Society for Microbiology, 1999.
- Foot, M.R.D. *SOE: An Outline History of the Special Operations Executive 1940–46*. London: British Broadcasting Corporation, 1984.
- Foot, Shelby. *The Civil War—A Narrative*. New York: Vintage Books/Random House, 1986.
- Ford, Harold P. *CIA and the Vietnam Policymakers: Three Episodes, 1962–1968*. Washington, D.C.: History Staff, Center for the Study of Intelligence, 1998.
- Ford, Harold P. *Estimative Intelligence: The Purposes and Problems of National Intelligence Estimating*. Lanham, MD: University Press of America, 1993.
- Foreign and Commonwealth Office Special Review Team. *List of Papers Released From the Previously Retained FCO Archive*. London: LRD, 1994. 2d ed. London: LRD, 1995.
- Foreign and Commonwealth Office. *Library and Records Department. Historical Branch. IRD: Origins and Establishment of the Foreign Office Information Research Department, 1946–8*. London: LRD/FCO, 1995.
- Forsberg, Randall. *Nonproliferation Primer: Preventing the Spread of Nuclear, Chemical, and Biological Weapons*. Cambridge, MA: MIT Press, 1995.
- Forster, Christopher F. *Environmental Biotechnology*. New York: John Wiley & Sons, 1987.
- Fowler, C.M.R. *The Solid Earth*. Cambridge: University Press, 1990.
- Fox, Nicols. *Spoiled: Why Our Food is Making Us Sick and What We Can Do About It*. New York: Penguin USA, 1998.
- Fox, Robert W., and Alan T. McDonald. *Introduction to Fluid Mechanics*. 5th ed. New York: John Wiley & Sons, 1998.
- Francis, Frederick. *Wiley Encyclopedia of Food Science and Technology*. New York: Wiley, 1999.
- Frank, Benis M. *U.S. Marines in Lebanon, 1982–1984*. Washington, D.C.: U.S. Marine Corps, 1987.

- Freedman, Maurice. *Unravelling Enigma: Winning the Code War at Station X*. Barnsley, South Yorkshire, England: Leo Cooper, 2000.
- Freeman, R. L. *Telecommunication System Engineering*. New York: Wiley, 1989.
- Freeze, R. A., and J. A. Cherry. *Ground Water*. Englewood Cliffs, NJ: Prentice-Hall, 1979.
- Freeze, R., and J. Cherry. *Groundwater*. Englewood Cliffs: Prentice-Hall, Inc., 1979.
- Freund, John E., and Richard Smith. *Statistics: a First Course*. Englewood Cliffs, NJ: Prentice Hall Inc., 1986.
- Fried, Bernard, and Joseph Sherma. *Thin-Layer Chromatography (Chromatographic Science, V. 81)*. New York: Marcel Dekker, 1999.
- Friedlander, S. K. *Smoke, Dust and Haze: Fundamentals of Aerosol Behavior*. New York: John Wiley & Sons, 1977.
- Friedman, J., F. Dill, M. Hayden, and B. McGillivray. *Genetics*. Maryland: Williams & Wilkins, Bantam, 1996.
- Friend, J. Newton. *Man and the Chemical Elements: An Authentic Account of the Successive Discovery and Utilization of the Elements From the Earliest Times to the Nuclear Age*. 2nd revised ed. New York: Charles Scribner's Sons, 1961.
- Frist, W.H. *When Every Moment Counts: What You Need to Know About Bioterrorism from the Senates only Doctor*. Lanham, MD: Rowman & Littlefield, 2002.
- Fritz, Sandy, and Jack Brown. *Understanding Germ Warfare (Science Made Accessible)*. New York: Warner Books, 2002.
- Fritz, W., and J. Moore. *Basics of Physical Stratigraphy and Sedimentology*. New York: John Wiley & Sons, 1988.
- Fuller, Buckminster. *Ideas and Integrity*. Toronto: Collier Books, 1963.
- Fursenko, Alexandr, and Timothy J. Naftali. *One Hell of a Gamble: Khrushchev, Castro, and Kennedy, 1958–1964*. New York: W. W. Norton and Company, 1998.
- Gaddis, John L. *The United States and the Origins of the Cold War*. rev. ed. New York: Columbia University Press, 2000.
- Gaddis, John L. *We Now Know: Rethinking Cold War History*. New York: Oxford University Press, 1997.
- Gaffney, Timothy, R. *Secret Spy Satellites: America's Eyes in Space*. Berkeley Heights, NJ: Enslow Publishers Inc., 2000.
- Gall, Carlotta, and Thomas De Waal. *Chechnya: Calamity in the Caucasus*. New York: New York University Press, 1998.
- Gallagher, Thomas Michael. *Assault in Norway: Sabotaging the Nazi Nuclear Bomb*. New York: Harcourt Brace Jovanovich, 1975.
- Gann, Ernest Kellogg. *The Black Watch: The Men Who Fly America's Secret Spy Planes*. New York: Random House, 1989.
- Ganong, W. F. *Review of Medical Physiology*, 16th ed. Prentice-Hall International, Inc., 1993.
- Gardner, Joan F., and Margaret M. Peel. *Introduction to Sterilization and Disinfection*. Melbourne: Churchill Livingstone, 1986.
- Gardner, Martin. *Codes, Ciphers, and Secret Writing*. New York: Pocket Books, 1974.
- Gardner, Robert. *Crime Lab 101: Experimenting with Crime Detection*. New York: Walker, 1992.
- Garrett, L. *The Coming Plague: Newly Emerging Diseases in a World out of Balance*. New York: Penguin Books, 1995.
- Gasman, Daniel. *Haeckel's Monism and the Birth of Fascist Ideology*. New York: Peter Lang, 1998.
- Gasman, Daniel. *The Scientific Origins of National Socialism: Social Darwinism in Ernst Haeckel and the German Monist League*. London: Macdonald, 1971.
- Gates, Robert M. *From the Shadows: The Ultimate Insider's Story of Five Presidents and How They Won the Cold War*. New York: Simon and Schuster, 1996.
- Gebhardt, James F. *Soviet Special Purpose Forces: An Annotated Bibliography*. Fort Leavenworth, KS: U.S. Army Combined Arms Center, Soviet Army Studies Office, May 1990.
- Gelfond, A.O. *Transcendental and Algebraic Numbers*. Dover Publications, 2003.
- Gellately, Robert. *The Gestapo and German Society*. Oxford: Oxford University Press, 1991.
- Gelman, Robert B. and Stanton McCandlish. *Protecting Yourself Online: The Definitive Resource on Safety, Freedom, and Privacy in Cyberspace*. New York: HarperEdge, 1998.
- George, John, and Laird Wilcox. *American Extremists: Militias, Supremacists, Klansmen, Communists, and Others*. Amherst, NY: Prometheus Books, 1996.
- Gerson, Allan, and Jerry Adler. *The Price of Terror*. New York: HarperPerennial, 2002.
- Gibson, David J. *Methods in Comparative Plant Population Ecology*. Oxford: Oxford University Press, 2002.
- Gilbert, Abby L. *A Historical Guide to the U.S. Government*. George T. Kurian, ed. New York and Oxford: Oxford University, 1998.
- Gilbert, James L., and John Patrick Finnegan. *U.S. Army Signals Intelligence in World War II: A Documentary History*. Washington, D.C.: U.S. Government Printing Office, 1993.
- Gilbert, Martin. *The First World War: A Complete History*. New York: Henry Holt, 1996.
- Gilderhus, Mark T. *The Second Century: U.S.-Latin American Relations Since 1889*. Wilmington, DE: Scholarly Resources, 2000.
- Gill, Arthur, Steve Krar, and Peter Smid. *Machine Tool Technology Basics*. New York: Industrial Press, 2002.
- Gillespie, Angus K. *Twin Towers: The Life of New York City's World Trade Center*. New Brunswick, NJ: Rutgers University Press, 1999.
- Gillies, James, and R. Cailliau. *How the Web Was Born: The Story of the World Wide Web*. New York: Oxford University Press, 2000.
- Gilligan, Tom. *CIA Life: 10,000 Days with the Agency*. Connecticut: Foreign Intelligence Press, 1991.
- Gilmour, Robert S., and Alexis A. Halley. *Who Makes Public Policy? The Struggle for Control Between Congress and the Executive*. Chatham, NJ: Chatham House Publishers, 1994.
- Gilpin, Alan. *Dictionary of Fuel Technology*. New York: Philosophical Library, 1969.
- Glasston, Samuel and Alexander Sesonske. *Nuclear Reactor Engineering: Vol. 1, Reactor Design Basics*. New York: Chapman & Hall, 1994.

- Glele, Jame. *Chaos: Making a New Science*. New York: Viking Penguin, Inc., 1988.
- Glick, B. R., and J. J. Pasternak. *Molecular Biotechnology, Principles and Applications of Recombinant DNA*, 2nd edition. Washington: American Society of Microbiology Press, 1998.
- Global Trends 2015: A Dialogue about the Future with Nongovernment Experts*. Langley, CA: National Intelligence Council, 2000.
- Godson, Roy. *Dirty Tricks or Trump Cards: U.S. Covert Action and Counterintelligence*. Washington: Brassey's, 1996.
- Godson, Roy. *United States Intelligence at the Crossroads: Agendas for Reform*. Washington: Brassey's, 1995.
- Godwin, Robert. *X-15: The NASA Mission Reports, Incorporating Files from the USAF*. Burlington, Ontario: Apogee Books, 2000.
- Göksu, H.Y., M. Oberhofer, and D. Regulla, Eds. *Scientific Dating Methods*. Boston: Kluwer Academic Publishers, 1991.
- Gold, Mark and Michael Boyette. *Wonder Drugs: How They Work*. New York: Simon & Schuster, 1987.
- Goldreich, Oded. *Foundations of Cryptography: Basic Tools*. Cambridge: Cambridge University Press, 2001.
- Goldsmith, Robert, and Donald Hayneman, eds. *Tropical Medicine and Parasitology*. Norwalk, CT: 1989.
- Goldstein, G., and M. Hersen, eds. *Handbook of Psychological Assessment*. 2nd ed. New York: Pergamon Press, 1990.
- Goldstein, Herbert, Charles P. Poole, and John L. Safko. *Classical Mechanics*. 3rd ed. New York: Prentice Hall, 2002.
- Goldstein, Martin, and Inge Goldstein. *The Refrigerator and the Universe: Understanding the Laws of Energy*. Harvard University Press, 1993.
- Goleniewski, Lillian. *Telecommunication Essentials*. Boston: Addison Wesley Professional, 2001.
- Golos, E.B. *Foundations of Euclidean and Non-Euclidean Geometry*. New York: Holt, Rinehart and Winston, 1968.
- Goodman and Gilman. *The Pharmacological Basis of Therapeutics*. 6th ed. New York: Macmillan, 1980.
- Goodman, H. Maurice. *Basic Medical Endocrinology*. 2nd ed. New York: Raven Press, 1994.
- Goodwin, Peter H. *Engineering Projects for Young Scientists*. New York: Franklin Watts, 1987.
- Gorbaty, Martin L., John W. Larsen, and Irving Wender, eds. *Coal Science*. New York: Academic Press, 1982.
- Gordon, Nathan J., William L. Fleisher, and C. Donald Weinberg. *Effective Interviewing and Interrogation Techniques*. New York: Academic Press, 2001.
- Gordievsky, Oleg, and Christopher Andrew. *KGB, The Inside Story of its Foreign Operations from Lenin to Gorbachev*. New York: Harper Collins, 1990.
- Gore, Albert. *Department of State and U.S. Information Agency: Accompanying Report of the National Performance Review*. Washington, D.C.: U.S. Government Printing Office, 1993.
- Gorman, Martyn L., and R. David Stone. *The Natural History of Moles*. Ithaca, NY: Comstock Publishing Associates, 1990.
- Gormley, Dennis. *Dealing with the Threat of Cruise Missiles*. New York: Oxford University Press for the International Institute for Strategic Studies, 2001.
- Gosling, F.G. *The Manhattan Project: Science in the Second World War*. U.S. Department of Energy, 1990.
- Gottschalk, Jack A. and Brian P. Flanagan. *Jolly Roger With an Uzi: The Rise and Threat of Modern Piracy*. Annapolis: Naval Institute Press, 2000.
- Gough, M. *Agent Orange: The Facts*. New York: Perseus Books, 1986.
- Gough, W., et al. *Vibrations and Waves*. 2nd ed. Englewood Cliffs, NJ: Prentice Hall, 1995.
- Goulden, Joseph C. *Korea, the Untold Story of the War*. New York: Times Books, 1982.
- Gowar, Norman. *An Invitation to Mathematics*. New York: Oxford University Press, 1979.
- Goyer, R.A. "Toxic Effects of Metals." *Casarett and Doull's Toxicology: The Basic Science of Poisons*, 5th edition. New York: McGraw-Hill Companies, Inc., 1996.
- Graebner, Norman A., ed. *The National Security: Its Theory and Practice, 1945–1960*. New York: Oxford University Press, 1986.
- Graetzer, Hans G., and David L. Anderson. *The Discovery of Nuclear Fission: A Documentary History*. New York: Van Nostrand Reinhold, 1971. Reprint: Arno Press, 1981.
- Graetzer, Hans G., and Larry M. Browning. *The Atomic Bomb: An Annotated Bibliography*. Pasadena: Salem Press, 1992.
- Grafe, A. *A History of Experimental Virology*. New York: Springer-Verlag, 1991.
- Graham, L. *Science in Russia and the Soviet Union*. Cambridge: Cambridge University Press, 1993.
- Grant, David, and Robin Harris. *Encyclopedia of Nuclear Magnetic Resonance*. New York: Wiley, 2003.
- Graves, Harold N. *On the Short Wave*. New York: Foreign Policy Association, 1941.
- Gray, Henry, Lawrence H. Bannister, Martin M. Berry, and Peter L. Williams, eds. *Gray's Anatomy: The Anatomical Basis of Medicine & Surgery*. London: Churchill Livingstone, 1995.
- Gray, J. *Man Against Disease-Preventive Medicine*. New York: Oxford University Press, 1979.
- Green, Michael. *Bomb Detection Squads*. Mankato, MN: Capstone Press, 1998.
- Green, Robert E. *Machinery's Handbook*. 24th ed. New York: Industrial Press, 1992.
- Greenwood, N. N. and A. Earnshaw. *Chemistry of the Elements*. New York: Butterworth-Heinemann, 1997.
- Gregg, Robert. *International Relations on Film*. Boulder, CO: Lynne Rienner Publishers, 1998.
- Gregory, B. *Inventing Reality: Physics as Language*. New York: John Wiley & Sons, 1990.
- Greider, William. *Secrets of the Temple: How the Federal Reserve Runs the Country*. New York: Simon and Schuster, 1987.
- Gribbin, John. *Q is for Quantum: An Encyclopedia of Particle Physics*. New York: The Free Press, 1998.
- Griffith, H. Winter. *Complete Guide to Prescription and Non-Prescription Drugs*. Los Angeles: The Body Press, 1991.
- Griffiths, A. et al. *Introduction to Genetic Analysis*, 7th ed. New York, W.H. Freeman and Co., 2000.

- Grigg, E.R.N. *The Trail of Invisible Light for X-Strahlen to Radiobiology*. Springfield, IL: Charles C. Thomas, 1965.
- Griswold, Terry, and D. M. Giangreco. *Delta, America's Elite Counterterrorist Force*. Osceola, WI: Motorbooks International, 1992.
- Grose, Peter. *Gentleman Spy: The Life of Allen Dulles*. Boston: Houghton Mifflin, 1994.
- Grose, Peter. *Operation Rollback: America's Secret War Behind the Iron Curtain*. Boston: Houghton-Mifflin, 2000.
- Gross, M. L., R. Caprioli, and P. B. Armentrout. *The Encyclopedia of Mass Spectrometry: Ion Chemistry and Theory*. Oxford: Pergamon Press, 2001.
- Groves, Donald G. and Lee M. Hunt. *Ocean World Encyclopedia*. New York: McGraw-Hill Book Company, 1980.
- Guide to Background Investigations: A Comprehensive Source Directory for Employee Screening and Background Investigations*. Tulsa, OK: T.I.S.I., 1998.
- Guilbert J.M., and C.F. Park. *The Geology of Ore Deposits*. W.H. Freeman, 1986.
- Gullberg, Jan, and Peter Hilton. *Mathematics: From the Birth of Numbers*. W.W. Norton & Company, 1997.
- Gundermann, K.D., and F. McCapra. *Chemiluminescence in Organic Chemistry*. New York: Springer-Verlag, 1987.
- Gunston, Bill. *The Development of Jet and Turbine Aero Engines*. 2nd ed. New York: Haynes Publishing, 1998.
- Guyton, A. C. *Human Physiology and Mechanisms of Disease*. 4th ed. Philadelphia: W.B. Saunders Co., 1987.
- Guyton, A.C., and J.E. Hall. *Textbook of Medical Physiology*, 10th ed. New York: W.B. Saunders Company, 2000.
- Haass, Richard, and Meghan L. O'Sullivan. *Honey and Vinegar: Incentives, Sanctions, and Foreign Policy*. Washington, D.C.: Brookings Institution Press, 2000.
- Haber-Schaim et. al. *Introductory Physical Science*. 5th ed. Englewood Cliffs, N.J.: Prentice-Hall, 1987.
- Hafner, Katie, and Matthew Lyon. *Where Wizards Stay Up Late: The Origins of the Internet*. New York: Simon & Schuster, 1996.
- Hafner, R.S. (Editor). "Transportation, Storage, and Disposal of Radioactive Materials: Presented at the 1999" *Asme Pressure Vessels and Piping Conference*. American Society of Mechanical Engineers, 1990.
- Hagen, Robert M., and James Trefil. *Science Matters*. New York: Doubleday, 1991.
- Hager, Nicky. *Secret Power*. Nelson, New Zealand: Craig Potton, 1996.
- Hahn, Liang-shin. *Complex Numbers and Geometry*. 2nd ed. The Mathematical Association of America, 1996.
- Haines, G.K., and R.E. Leggett, eds. *CIA's Analysis of the Soviet Union 1947-1991*. Washington, D.C.: CIA History Staff, Center for the Study of Intelligence, 2001.
- Halberstam, David. *New York September 11*. New York: Power-House Books, 2001.
- Haldane, Robert A. *The Hidden War*. New York: St. Martin's, 1978.
- Hamblin, W.K., and E.H. Christiansen. *Earth's Dynamic Systems*. 9th ed. Upper Saddle River: Prentice Hall, 2001.
- Hammel, Eric M. *The Root: The Marines in Beirut, August 1982-February 1984*. San Diego: Harcourt Brace Jovanovich, 1985.
- Hammond, Thomas Taylor, comp. and ed. *Soviet Foreign Relations and World Communism: A Selected, Annotated Bibliography of 7,000 Books in 30 Languages*. Princeton, NJ: Princeton University Press, 1965.
- Hamzah, Khidr Ald Al-Abbis, and Jeff Stein. *Saddam's Bombmaker: The Terrifying Inside Story of the Iraq Nuclear and Biological Weapons Agenda*. New York: Scribner, 2002.
- Han, Jiawei, and Micheline Kamber. *Data Mining: Concepts and Techniques*. New York: Morgan Kaufmann Publishers, 2000.
- Han, M.Y. *The Probable Universe*. Blue Ridge Summit, PA: TAB Books, 1993.
- Hancock P. L. and B. J. Skinner, eds. *The Oxford Companion to the Earth*. Oxford: Oxford University Press, 2000.
- Handberg, Roger. *Ballistic Missile Defense and the Future of American Security: Agendas, Perceptions, Technology and Policy*. Westport, CT: Praeger, 2002.
- Haney, Eric L. *Inside Delta Force: The Story of America's Elite Counterterrorist Unit*. New York: Delacorte Press, 2002.
- Harden, Victoria Angela. *Rocky Mountain Spotted Fever: History of a Twentieth-Century Disease*. Baltimore: Johns Hopkins University Press, 1990.
- Hardy, Anne. *The Epidemic Streets: Infectious Diseases and the Rise of Preventive Medicine, 1956-1900*. New York: Oxford University Press, 1993.
- Hardy, M. J. *Sea, Sky, and Stars: An Illustrated History of Grumman Aircraft*. New York: Sterling, 1987.
- Hardy, Ralph, Peter Wright, John Kington, and John Gribben. *The Weather Book*. Boston: Little, Brown and Co., 1982.
- Hariharan, P. *Basics of Interferometry*. San Diego: Academic Press, 1992.
- Harper, David R., and Andrea S. Meyer. *Of Mice, Men, and Microbes: Hantavirus*. San Diego: Academic Press, 1999.
- Harper, Richard H.R. *Inside the IMF*. San Diego, CA: Academic Press, 1998.
- Harrelson, Leonard. *Lietest: Deception, Truth and the Polygraph*. Ft. Wayne, Indiana: Jonas Publishing, 1998.
- Harris, Cyril. *Handbook of Noise Control*. New York: McGraw Hill, 1979.
- Harris, Daniel C. *Quantitative Chemical Analysis*. 4th ed. New York: W.H. Freeman & Company, 1995.
- Harris, Robert, and Jeremy Paxman. *A Higher Form of Killing: The Secret History of Chemical and Biological Warfare*. New York: Random House, 2002.
- Harris, William R. *Intelligence and National Security: A Bibliography with Selected Annotations*. Rev. ed. Cambridge, MA: Harvard University, Center for International Affairs, 1968.
- Harrison, Maureen, and Steve Gilbert. *Landmark Decisions of the United States Supreme Court*. Beverly Hills, CA: Excellent Books, 1991.
- Hartcup, Guy. *Camouflage: A History of Concealment and Deception in War*. New York: Scribner's, 1980.
- Hartl, Daniel L. *Genetics*. Boston: Jones and Bartlett, 1994.

- Hastie, T., et al. *The Elements of Stastical Learning: Data Mining, Inference, and Prediction*. New York: Springer Verlag, 2001.
- Hastings, Max. *The Korean War*. New York: Simon and Schuster, 1987.
- Haugen, David M. *Biological and Chemical Weapons*. San Diego: Greenhaven Press, 2001.
- Hawley, Gessner G. *The Condensed Chemical Dictionary*. New York: Van Nostrand Reinhold Company, 9th edition, 1977.
- Hayat, M. Arif. *Microscopy, Immunohistochemistry, and Antigen Retrieval Methods for Light and Electron Microscopy*. New York: Plenum Publishing, 2002.
- Haydock, Michael D. *City Under Siege: The Berlin Blockade and Airlift, 1948–1949*. Washington, D.C.: Brassey's, 2000.
- Haynes, John Earl, and Harvey Klehr. *Venona: Decoding Soviet Espionage in America*. New Haven, Conn: Yale University Press, 1999.
- Heath, R. *Basic Ground-Water Hydrology*. U.S. Geological Survey Water-Supply Paper 2220, 1983.
- Hebra, Alexius J. *Measure for Measure: The Story of Imperial, Metric, and Other Units*. Baltimore: Johns Hopkins University Press, 2003.
- Hecht, Jeff. *Laser Pioneers*. New York: Academic Press, 1992.
- Hecht, Jeff. *Understanding Lasers*. New York: IEEE Press, 1994.
- Heiserman, D. L. *Exploring the Chemical Elements and Their Compounds*. Blue Ridge Summit, PA: Tab Publications, 1992.
- Helgeson, John. *Getting to Know the President: CIA Briefings of Presidential Candidates*, Washington, DC: Center for Study of Intelligence, CIA, 1995.
- Hellemans, Alexander and Bryan Bunch. *The Timetables of Science: A Chronology of the Most Important People and Events in the History of Science*. New York: Simon & Schuster Inc., 1988.
- Helms, Harry L. *Shortwave Listening Guidebook: The Complete Guide to Hearing the World*. Solana Beach, CA: High Text Publications, 1993.
- Hemond, H. F., and E. J. Fechner. *Chemical Fate and Transport in the Environment*. San Diego: Academic Press, 1994.
- Henderson, D.A., and T.V. Inglesby. *Bioterrorism: Guidelines for Medical and Public Health Management*. Chicago: American Medical Association, 2002.
- Henderson, Harry. *Privacy in the Information Age*. New York: Facts on File, 1999.
- Hendrickson, Robert. *The Ocean Almanac*. Garden City, New York: Doubleday and Company, 1984.
- Henne, P. A. *Applied Computational Aerodynamics*. Washington, D.C.: American Institute of Aeronautics and Astronautics, 1990.
- Hennessy, Thomas F. *Early Locks and Lockmakers of America*. Des Plaines, IL: Nickerson & Collins Pub. Co., 1976.
- Herken, Gregg. *Cardinal Choices: Presidential Science Advising from the Atom Bomb to SDI*. Stanford, CA: Stanford University Press, 2000.
- Herman, R. *Fusion: The Search for Endless Energy*. Oxford: Cambridge University Press, 1990.
- Hermann, Armin, et al. *History of CERN*. Amsterdam: North-Holland Physics Publishing, 1987.
- Hersch, Reginald, and Rhodes Fairbridge, eds. *Encyclopedia of Hydrology and Water Resources*. Boston: Kluwer Academic Publishing, 1998.
- Hersh, Burton. *The Old Boys: The American Elite and the Origins of the CIA*. New York: Charles Scribner's Sons, 1992.
- Heuer, Richards J., Jr. *Psychology of Intelligence Analysis*. Washington, D.C.: Center for the Study of Intelligence, 2000.
- Hewitt, Christopher. *Understanding Terrorism in America*. New York: Routledge, 2002.
- Hewitt, Steven. *Spying 101: The RCMP's Secret Activities at Canadian Universities*. Toronto: University of Toronto Press, 2002.
- Heyman, D.A., J. Achterberg, and J. Laszlo. *Lessons from the Anthrax Attacks: Implications for U.S. Bioterrorism Preparedness: A Report on a National Forum on Biodefense*. Washington, DC: Center for Strategic and International Studies, 2002.
- Heymann, Philip B. *Terrorism and America: A Commonsense Strategy for a Democratic Society*. Cambridge, Mass.: MIT Press, 1998.
- Hidy, G. M. "Aerosols." *Encyclopedia of Physical Science and Technology*. Edited by Robert A. Meyers. San Diego: Academic Press, 1987.
- Hillen, John. *Future Visions for U.S. Defense Policy: Four Alternatives Presented as Presidential Speeches*. New York: Council on Foreign Relations, 1998.
- Hilliard, Robert L. *The Federal Communications Commission: A Primer*. Boston: Focal Press, 1991.
- Hillman, Richard S., John A. Peeler, and Elsa Cardozo da Silva. *Democracy and Human Rights in Latin America*. Westport, CT: Praeger, 2002.
- Hinds, William C. *Aerosol Technology: Properties, Behavior, and Measurement of Airborne Particles*. 2nd ed. Hoboken, NJ: Wiley-Interscience, 1999.
- Hinsley, F. H., et al. *British Intelligences in the Second World War: Its Influence on Strategy and Operations*, Volume Three, Part I. London: Her Majesty's Stationary Office 1984.
- Hinsley, F.H. and Alan Stripp, eds. *Codebreakers: The Inside Story of Bletchley Park*. Oxford: Oxford University Press, 2001.
- Hinsley, F.H. *British Intelligence in the Second World War*. Cambridge: Cambridge University Press, 1988.
- Hiscox, G.D. *Mechanical Movements, Powers, and Devices*. New York: Norman W. Henley Publishing Co., 1927.
- History of the Bureau of Engraving and Printing, 1862–1962*. Washington, D.C.: Treasury Department, 1964.
- Ho, M.W. *Genetic Engineering Dream or Nightmare? The Brave New World of Bad Science and Big Business*, Dublin: Gateway, Gill & Macmillan, 1998.
- Hobbs, A. C. *The Construction of Locks*. West Orange, New Jersey: A. Saifer, 1982.
- Hobbs, Peter V., and M. Patrick McCormick, eds. *Aerosols and Climate*. Hampton, VA: A. Deepak, 1988.
- Hobson, Art. *Physics: Concepts and Connections*. Upper Saddle River, NJ: Prentice Hall, 1994.
- Hodgman, Charles D., Editor. *C. R. C. Standard Mathematical Tables*. Cleveland: Chemical Rubber Publishing Co, 1959.
- Hodgson, Michael, and Devin Wick. *Basic Essentials: Weather Forecasting*. 2nd ed. Guilford, CT: Globe Pequot Press, 1999.



- Hoehling, A.A. *The Great Epidemic*. Boston: Little, Brown and Company, 1961.
- Hoffman, Lance J. *Rogue Programs: Viruses, Worms, and Trojan Horses*. New York: Van Nostrand Reinhold, 1990.
- Hoffman, Lance J., ed. *Building in Big Brother: The Cryptographic Policy Debate*. New York: Springer-Verlag, 1995.
- Hoffmann, Peter, and Tom Harkin. *Tomorrow's Energy: Hydrogen, Fuel Cells, and Prospects for a Cleaner Planet*. Boston: MIT Press, 2001.
- Hogan, Michael H. *A Cross of Iron: Harry S. Truman and the Origins of the National Security State, 1945–1954*. Cambridge: Cambridge University Press, 1998.
- Hoge, James F., and Gideon Rose. *How Did This Happen?: Terrorism and the New War*. New York: Public Affairs, 2001.
- Hogg, R. V., and E. A. Tanis. *Probability and Statistical Inference*, 6th ed. New Jersey: Prentice Hall, Inc., 2001.
- Holder, William G. *Boeing B-52 Stratofortress*. Blue Ridge Summit, PA: AERO, 1988.
- Hollien, Harry Francis. *Forensic Voice Identification*. New York: Academic Press, 2001.
- Hollien, Harry Francis. *The Acoustics of Crime: The New Science of Forensic Acoustics*. New York: Plenum Press, 1990.
- Holloway, David. *Stalin and the Bomb: The Soviet Union and Atomic Energy, 1939–1954*. New Haven, Conn.: Yale University Press, 1994.
- Holme, David J., and Hazel Peck. *Analytical Biochemistry*. Essex, England: Burnt Mill, Harlow, 1993.
- Holmes, Ronald M. *Profiling Violent Crimes: An Investigative Tool*. Newbury Park, England: Sage Publications, 1989.
- Holmes, W. J. *Double-Edged Secrets: U.S. Naval Intelligence Operations in the Pacific During World War II*. Annapolis, MD: Naval Institute Press, 1979.
- Holmes-Siedle, Andrew. *Handbook of Radiation Effects*. New York: Oxford University Press, 1993.
- Holober, Frank. *Raiders of the China Coast: CIA Covert Operations during the Korean War (Special Warfare Series)*. Annapolis, MD: Naval Institute Press, 1999.
- Holton, James R. *An Introduction to Dynamic Meteorology*. 2nd ed. New York: Academic Press, 1979.
- Holtzman, Eric, and Alex B. Novikoff. *Cells and Organelles*. Philadelphia: Saunders College Publishing, 1984.
- Holum, John R. *Fundamentals of General, Organic and Biological Chemistry*. Wiley and Sons, 1994.
- Holzmann, Gerald J., and Bjorn Pehrson. *The Early History of Data Networks*. Los Alamitos, CA: IEEE Computer Society Press, 1995.
- Hood, William. *Mole: The True Story of the First Russian Intelligence Officer Recruited by the CIA*. New York: W.W. Norton, 1982.
- Hopkins, D.R. *The Greatest Killer: Smallpox in History*. Chicago: University of Chicago Press, 2002.
- Hopkins, Donald R. *Princes and Peasants, Smallpox in History*. Chicago: The University of Chicago Press, 1983.
- Hopkirk, Peter. *The Great Game: The Struggle for Empire in Central Asia*. New York: Kodansha International 1994.
- Hopla, C.E., and A.K. Hopla. "Tularemia" *Handbook of Zoonoses*. Boca Raton: CRC Press, 1994.
- Hopple, Gerald W., and Bruce W. Watson. *The Military Intelligence Community*. Boulder, CO: Westview Press, 1986.
- Horeh, Joshua. *An Iraqi Jew in the Mossad: Memoir of an Israeli Intelligence Officer*. Jefferson, NC: McFarland & Co., 1997.
- Horn, Delton E. *DAT: The Complete Guide to Digital Audio Tape*. Blue Ridge Summit, PA: TAB Books, 1991.
- Horne, James. *Why We Sleep: The Functions of Sleep in Humans and Other Mammals*. Oxford: Oxford University Press, 1988.
- Horowitz, Yigal S., ed. *Thermoluminescence and Thermoluminescent Dosimetry, Vol I and II*. Boca Raton, FL: CRC Press Inc., 1984.
- Houde, John. *Crime Lab: A Guide for Nonscientists*. Rolling Bay: Calico Press, 1998.
- Houghton, John. *The Physics of Atmospheres*. 3rd ed. Cambridge: Cambridge University Press, 2002.
- Houglum, Roger J. *Electronics: Concepts, Applications and History*. 2nd ed. Albany, NY: Delmar Publishers, 1985.
- Hoxie, R. Gordon et al. *The Presidency and National Security Policy*. New York: Center for the Study of the Presidency, 1984.
- Hubel, David H. *Eye, Brain, and Vision*. New York: Scientific American Library, 1988.
- Hudson, John. *The History of Chemistry*. New York: Chapman & Hall, 1992.
- Hughes, S. *The Virus: A History of the Concept*. New York: Science History Publications, 1977.
- Huisken, Ronald. *The Origin of the Strategic Cruise Missile*. New York: Praeger Publishers, 1981.
- Huizenga, John R. *Cold Fusion: The Scientific Fiasco of the Century*. Oxford: Oxford University Press, 1993.
- Hunt, Michael H. *Lyndon Johnson's War: America's Cold War Crusade in Vietnam, 1945–1968*. New York: Hill and Wang, 1996.
- Ignatius, David. *Agents of Innocence*. New York: W. W. Norton, 1987.
- Imagery Intelligence*. Washington, D.C.: Department of the Army, 1996.
- Immermann, Richard H. *John Foster Dulles and the Diplomacy of the Cold War*. Princeton, NJ: Princeton University Press, 1990.
- Incropera, Frank P., and David P. DeWitt. *Fundamentals of Heat and Mass Transfer*, 5th ed. New York: John Wiley & Sons, 2001.
- Ingamells, C. O., and Francis F. Pitard. *Applied Geochemical Analysis*. New York, NY: Wiley, 1986.
- Inglesby, Thomas V. "Bioterrorist Threats: What the Infectious Disease Community Should Know about Anthrax and Plague." *Emerging Infections 5*. Washington, DC: American Society for Microbiology Press, 2001.
- Ingram, Edward. *The Beginning of the Great Game in Asia: 1828–1834*. Oxford: Clarendon, 1979.
- INR, Intelligence and Research in the Department of State*. Washington, D.C.: Bureau of Intelligence and Research, 1983.

- Institute of Medicine. *Assessment of Future Scientific Needs for Live Variola Virus*. Washington, DC: National Academy Press, 1999.
- Intelligence Agencies: Personnel Practices at CIA, NSA, and DIA Compared with Those of Other Agencies*. Washington, D.C.: General Accounting Office, 1996.
- Interrante, Leonard V. *Chemistry of Advanced Materials: An Overview*. Vch Publishing, 1997.
- Irvin, Victor D. *Political Assassination: The Strategic Precision Weapon of Choice*. Carlisle Barracks, PA: U.S. Army War College, 2002.
- Isselbacher, Kurt J., et al. *Harrison's Principles of Internal Medicine*. New York: McGraw-Hill, 1994.
- Isser, Harel. *The House on Garibaldi Street: The First Full Account of the Capture of Adolf Eichmann*. New York: Viking Press, 1975.
- Jacobs, George, and Theodore J. Cohen. *The Shortwave Propagation Handbook*. Cowan Publishing Corp., 1970.
- Jahn, F., M. Cook, and M. Graham. *Hydrocarbon Exploration and Production. Developments in Petroleum Science*. The Netherlands: Elsevier Science, 2000.
- James, I. N. *Introduction to Circulating Atmospheres*. New York: Cambridge University Press, 1994.
- James, Lawrence. *Raj: The Making and Unmaking of British India*. New York: St. Martin's Griffin, 1997.
- Janseen, Marc, and Nikita Petrov. *Stalin's Loyal Executioner: People's Commissar Nikolai Ezhov 1895–1940*. Palo Alto, CA: Hoover Institution Press, 2002.
- Jeffrey-Jones, Rhodri. *The CIA and American Democracy*. New Haven: Yale University Press, 1991.
- Jeffreys-Jones, Rhodri, and Christopher M. Andrew. *Eternal Vigilance? 50 Years of the CIA*. Portland, OR: Frank Cass, 1997.
- Jeffreys-Jones, Rhodri. *Cloak and Dollar: A History of American Secret Intelligence*. New Haven, CT: Yale University Press, 2002.
- Jenkins, Brian Michael. *The Lessons of Beirut: Testimony Before the Long Commission*. Santa Monica, CA: Rand Corporation, 1984.
- Jenkins, Dennis R. *Lockheed Secret Projects: Inside the Skunk Works*. St. Paul, MN: MBI Publishing, 2001.
- Jenkins, F.A. and H.E. White. *Fundamentals of Optics*. New York: McGraw-Hill, 1976.
- Jenner, Edward, Herve Bazin, Andrew Morgan, and Glenise Morgan, trans. *The Eradication of Small Pox: Edward Jenner and the First and Only Eradication of a Human Infectious Disease*. San Diego: Academic Press, 2000.
- Jerrard, H. G., and D. B. McNeil. *A Dictionary of Scientific Units: Including Dimensionless Numbers and Scales*. London: Chapman and Hall, 1980.
- Joellenbeck, L.M., L.L. Zwanziger, J.S. Durch, et al. *The Anthrax Vaccine: Is It Safe? Does It Work?* Washington, DC: National Academies Press, 2002.
- Joesten, Melvin D., David O. Johnston, John T. Netterville, and James L. Wood. *World of Chemistry*. Belmont, CA: Brooks/Cole Publishing Company, 1995.
- Johnson, C. K., with M. Smith. *More Than My Share of it All*. Washington, DC: Smithsonian Institution Press, 1985.
- Johnson, Eric R. *Servomechanisms*. New York: Prentice-Hall, Inc., 1996.
- Johnson, Loch K. *Secret Agencies: U.S. Intelligence in a Hostile World*. New Haven, CT: Yale University Press, 1996.
- Johnson, Loch K. *The Central Intelligence Agency: History and Documents*. New York: Oxford University Press, 1989.
- Johnson, Robert Erwin. *Guardians of the Sea: History of the United States Coast Guard, 1915 to the Present*. Annapolis: Naval Institute Press, 1987.
- Johnson, William, with Jack Maguire. *Who's Stealing Your Business? : How to Identify and Prevent Business Espionage*. New York: AMACOM, American Management Association, 1998.
- Joneja, Janice V., and Leonard Bielory. *Understanding Allergy, Sensitivity, and Immunity*. New Brunswick: Rutgers University Press, 1990.
- Jones, Dwight V., and Richard F. Shea. *Transistor Audio Amplifiers*. New York: John Wiley & Sons, 1968.
- Jones, Joseph. *Stealth Technology*. Blue Ridge Summit, PA: TAB Books, 1994.
- Jones, P. M., ed. *Nuclear Power: Policy and Prospects*. New York: John Wiley & Sons, 1987.
- Joravsky, D. *The Lysenko Affair*. Cambridge, Massachusetts: Harvard University Press, 1970.
- Jorde, L. B., J. C. Carey, M. J. Bamshad, and R. L. White. *Medical Genetics*. 2nd ed. Mosby-Year Book, Inc., 2000.
- Jorgensen, E. P., ed. *The Poisoned Well: New Strategies for Groundwater Protection*. Washington, DC: Island Press, 1989.
- Jorgenson, Finn. *The Complete Handbook of Magnetic Recording*. 4th ed. New York: McGraw-Hill Professional Book Group, 1995.
- Joseph, Robert G., and John F. Reichart. *Deterrence and Defense in a Nuclear, Biological, and Chemical Environment*. Washington, D.C.: Center for Counterproliferation Research, National Defense University, 1999.
- Jowett, Garth S., and Victoria O'Donnell. *Propaganda and Persuasion*. Thousand Oaks, CA: Sage Publications, 1999.
- Judah, Tim. *Kosovo: War and Revenge*. New Haven, CT: Yale University Press, 2000.
- Juergensmeyer, Mark. *Terror in the Mind of God: The Global Rise of Religious Violence*. Berkeley: University of California Press, 2000.
- Julitte, Pierre. *Block 26: Sabotage at Buchenwald*. Garden City, NY: Doubleday, 1971.
- Jussim, Daniel. *Drug Tests and Polygraphs*. New York: Julian Messner, A Division of Simon & Schuster, Inc., 1987.
- Kahaner, Larry. *Competitive Intelligence: From Black Ops to Boardrooms: How Businesses Gather, Analyze, and Use Information to Succeed in the Global Marketplace*. New York: Simon & Schuster, 1996.
- Kahn, David. *The Codebreakers: The Story of Secret Writing*. New York: MacMillan Publishing Co., Inc., 1967.
- Kahn, David. *Kahn on Codes: Secrets of the New Cryptology*. New York: Macmillan, 1983.

- Kahn, David. *The Code-Breakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. New York: Scribner, 1997.
- Kaku, Michio, and Jennifer Trainer. *Nuclear Power, Both Sides: The Best Arguments For and Against the Most Controversial Technology*. New York: W. W. Norton, 1982.
- Kalpakjian, Serope. *Manufacturing Processes for Engineering Materials*. New York: Addison-Wesley Publishing Company, 1991.
- Kalugin, Oleg. *The First Directorate: My 32 Years in Intelligence and Espionage against the West*. New York: St. Martin's Press, 1994.
- Karagozian, A. R. "Jet Propulsion." *Encyclopedia of Physical Science and Technology*. Edited by Robert A. Meyers. Orlando, FL: Academic Press, 1987.
- Karush, William. *Dictionary of Mathematics*. Webster's New World Printing, 1989.
- Katz, Barry M. *Foreign Intelligence: Research and Analysis in the Office of Strategic Services, 1942–1945*. Cambridge, MA: Harvard University Press, 1989.
- Katz, Bernard S. C., and Daniel Vencill, eds. *Biographical Dictionary of the United States Secretaries of the Treasury, 1789–1995*. Westport, CT: Greenwood, 1996.
- Katz, Samuel M. *Relentless Pursuit: The DSS and the Manhunt for the al-Qaeda Terrorists*. New York: Tom Doherty Associates, 2002.
- Kaufman, Charles, et. el. *Network Security: Private Communication in a Public World*, 2nd. ed. Upper Saddle River, NJ: Prentice Hall, 2002.
- Kaufman, Yogi. *City at Sea*. Annapolis, MD: Naval Institute Press, 1995.
- Kay, Sean. *NATO and the Future of European Security*. Lanham, Maryland: Rowman and Littlefield, 1998.
- Keaney, Thomas A. *Strategic Bombers and Conventional Weapons: Airpower Options*. Washington, D.C.: National Defense University Press, 1984.
- Keegan, John. *A History of Warfare*. New York: Alfred A. Knopf, 1994.
- Keeton, William T., and James L. Gould. *Biological Science*. New York: W.W. Norton and Co., 1993.
- Keller, Peter A. *The Cathode-Ray Tube: Technology, History, and Applications*. Palisades Press, 1992.
- Kelling, George L. *Broken Windows and Police Discretion*. Washington, D.C.: National Institute of Justice, 1999.
- Kelly, John F., and Phillip K. Wearne. *Tainting Evidence: Inside the Scandals at the FBI Crime Lab*. New York: Free Press, 1998.
- Kelly, Saul, and Anthony Gorst. *Whitehall and the Suez Crisis*. Portland, OR: Frank Cass, 2000.
- Kendrew, J., et al. *The Encyclopedia of Molecular Biology*. Oxford: Blackwell Science Ltd., 1994.
- Kennon, Patrick E. *The Twilight of Democracy*. New York: Doubleday, 1995.
- Kent, Anthony. *Experimental Low-Temperature Physics*. New York: American Institute of Physics, 1993.
- Kent, Sherman. *Strategic Intelligence for American World Policy*. Princeton: Princeton University Press, 1966.
- Kessler, Ronald. *Escape from the CIA*. New York: Pocket Books, 1991.
- Kessler, Ronald. *Inside the CIA: Revealing the Secrets of the World's Most Powerful Spy Agency*. New York: Pocket Books, 1992.
- Kevles, Bettyann Holtzmann. *Medical Imaging in the Twentieth Century*. Rutgers University Press, 1996.
- Keynes, Milton. *Handling Laboratory Microorganisms*. Philadelphia: Open University Press, 1991.
- Khan, David. *The Codebreakers: The Story of Secret Writing*. New York: Scribner, 1996.
- Khan, Munawwar. *Anglo-Afghan Relations, 1798–1878: A Chapter in the Great Game in Central Asia*. Khyber Bazar-Peshawar: University Book Agency, 1963.
- Kim, Jin-hyun, and Chung-in Moon. *Post-Cold War, Democratization, and National Intelligence: A Comparative Perspective*. Seoul: Yonsei University Press, 1996.
- Kingslake, Rudolph. *A History of the Photographic Lens*. New York: Academic Press, 1989.
- Kippenhahn, Rudolf. *Code Breaking: A History and Exploration*. Woodstock, NY: Overlook Press, 1999.
- Kirk-Othmer. *Encyclopedia of Chemical Technology*. New York: Wiley, 1991.
- Kirkpatrick, Lyman B. *The U.S. Intelligence Community: Foreign Policy and Domestic Activities*. New York: Hill and Wang, 1973.
- Kish, John, and David Turns. *International Law and Espionage*. Boston: M. Nijhoff Publishers, 1995.
- Kissinger, Henry. *Problems of National Strategy: A Book of Readings*. New York: Praeger, 1965.
- Kissinger, Henry. *Years of Renewal*. New York: Simon and Schuster, 1999.
- Kissinger, Henry, and Clare Boothe Luce. *White House Years*. Boston: Little, Brown, 1979.
- Kittel, Charles. *Introduction to Solid State Physics*. New York: John Wiley & Sons, 1996.
- Klaassen, Curtis D. *Casarett and Doull's Toxicology*. 6 th ed. Columbus: McGraw-Hill, Inc., 2001.
- Klass, D.L. *Biomass for Renewable Energy, Fuels, and Chemicals*. Academic Press, 1998.
- Klein, C. *The Manual of Mineral Science*. 22nd ed. New York: John Wiley & Sons, Inc., 2002.
- Klein, Herbert A. *The Science of Measurement*. New York: Dover, 1974.
- Klug, William S., and Michael R. Cummings. *Concepts of Genetics*. 5th ed. Upper Saddle River, NJ: Prentice-Hall, Inc., 1997.
- Knapp, Rebecca, et al. *Clinical Epidemiology and Biostatistics*. Baltimore: Williams & Wilkins, 1992.
- Knezys, Stasys, and Romanas Sedlickas. *The War in Chechnya*. College Station: Texas A&M University Press, 1999.
- Knight, Amy. *Beria: Stalin's First Lieutenant*. Princeton, NJ: Princeton University Press, 1996.
- Knott, Stephan F. *Secret and Sanctioned-Covert Operations and the American Presidency*. New York: Oxford University Press, 1996.

- Kobayashi, G., Patrick R. Murray, Ken Rosenthal, and Michael Pfaller. *Medical Microbiology*. St. Louis, MO: Mosby, 2003.
- Koch, A.L. *Bacterial Growth and Form*. Dordrecht: Kluwer Academic Publishers, 2001.
- Koch, S., and B.D. Fila. *Our First Line of Defense, Presidential Reflections*. Washington, D.C.: Center for the Study of Intelligence, 1996.
- Koehler, T.M. *Anthrax*. Berlin: Springer Verlag, 2002.
- Kohler, John O. *Stasi: The Untold Story of the East German Secret Police*. Boulder, Colorado: Westview Press, 1999.
- Kondepudi, Dilip, and Ilya Prigogine. *Modern Thermodynamics: From Heat Engines to Dissipative Structures*. New York: John Wiley & Sons, 1998.
- Koneman, E., et al., eds. *Color Atlas and Textbook of Diagnostic Microbiology*, 4th ed. Philadelphia: J. B. Lippincott, 1992.
- Koneman, Elmer W. *Color Atlas and Textbook of Diagnostic Microbiology*. 4th ed. Philadelphia: J. B. Lippincott, 1992.
- Konheim, Alan G. *Cryptography: A Primer*. New York: Wiley, 1981.
- Kornbluh, Peter. *Bay of Pigs Declassified: The Secret CIA Report on the Invasion of Cuba*. New York: New Press, 1998.
- Kozaczuk, Wladyslaw. *Enigma: How the German Machine Cipher was Broken, and How It was Read by the Allies in World War Two*. Frederick, MD: University Publications of America, 1984.
- Kozlow, Christopher, and John P. Sullivan. *Jane's Facility Security Handbook*. Alexandria, VA: Jane's Information Group, 2000.
- Krasner, R.I. *The Microbial Challenge: Human-Microbe Interactions*. Washington: American Society for Microbiology, 2002.
- Krauskopf, K.B. *Introduction to Geochemistry*. New York: McGraw Hill, 1995.
- Kreis, John F. *Piercing the Fog: Intelligence and Army Air Forces Operations in World War II*. Washington, D.C.: Air Force History and Museums Program, 1996.
- Krepon, Michael. *Commercial Observation Satellites and International Security*. New York: St. Martin's Press, 1990.
- Krug, R.M., J.S. Flint, L.W. Enquist, V.R. Racaniello, and A.M. Skalka. *Principles of Virology*. Washington: American Society for Microbiology, 1999.
- Kruse, Warren G., II., and Jay G. Heiser. *Computer Forensics: Incident Response Essentials*. Boston: Addison Wesley Professional, 2001.
- Kuhns, Woodrow J. *Assessing the Soviet Threat: The Early Cold War Years*. Washington, D.C.: Center for the Study of Intelligence, 1997.
- Kunz, Diane B. *The Economic Diplomacy of the Suez Crisis*. Chapel Hill: University of North Carolina Press, 1991.
- Kupperberg, Paul. *Spy Satellites (The Library of Satellites)*. New York: Rosen Publishing Group, 2003.
- Kurstak, Edouard, ed. *Control of Virus Diseases*. New York: Marcel Dekker, 1993.
- Kyle, Keith. *Suez*. New York: St. Martin's Press, 1991.
- La Feber, Walter. *America, Russia, and the Cold War*. McGraw-Hill Humanities, 2001.
- Lake, Jon. *Jane's How to Fly and Fight in the F-117A Stealth Fighter*. London: HarperCollins Publishers, 1997.
- Lance, Simpson L., ed. *Botulinum Neurotoxin and Tetanus Toxin*. San Diego: Academic Press, 1989.
- Landau, Alan M., et. al. *U.S. Special Forces: Airborne Rangers, Delta, and U.S. Navy SEALs*. Osceola, WI: MBI, 1999.
- Landesman, Linda Young. *Public Health Management of Disasters: The Practical Guide*. Washington, D.C.: American Public Health Association, 2001.
- Lanza, Robert P., Robert Langer, and Joseph P. Vacanti. *Principles of Tissue Engineering*. Academic Press, 2000.
- Larish, John J. *Electronic Photography*. Blue Ridge Summit, PA: TAB Professional and Reference Books, 2000.
- Lashmar, Paul. *Spy Flights of the Cold War*. Great Britain: Sutton Publishing Limited, 1996.
- Lasnier, F. and T. Gan Ang. *Photovoltaic Engineering Handbook*. Bristol, England: IOP Publishing, 1990.
- Launius, Roger D. *Innovation and the Development of Flight*. College Station: Texas A&M University Press, 1999.
- Laurence, Clifford L. *The Laser Book*. Englewood Cliffs, NJ: Prentice Hall, 1986.
- Lavoy, Peter R., Scott D. Sagan, and James J. Wirtz. *Planning the Unthinkable: How New Powers Will Use Nuclear, Biological, and Chemical Weapons*. Cornell: Cornell University Press, 2001.
- Layton, Peggy Diane. *Emergency Food Storage & Survival Handbook: Everything You Need to Know to Keep your Family Safe in a Crisis*. Roseville, CA: Prima Publishing, 2002.
- Leary, William M. ed. *The Central Intelligence Agency: History and Documents*. Tuscaloosa, AL: University of Alabama Press, 1984.
- Lebow, Eileen F. *A Grandstand Seat: The American Balloon Service in World War I*. Westport, CT: Praeger, 1998.
- Lechevalier, Herbert A., and Morris Solotorovsky, eds. *Three Centuries of Microbiology*. Columbus: McGraw-Hill, 1965.
- Lederberg, Joshua, and William S. Cohen. *Biological Weapons: Limiting the Threat (BCSIA Studies in International Security)*. Boston: MIT Press, 1999.
- Ledwidge, Michael S. *Bas Connection*. New York: Simon & Schuster, 2001.
- Leffler, Melvyn P. *A Preponderance of Power: National Security, the Truman Administration, and the Cold War*. Stanford, CA: Stanford University Press, 1992.
- Legislative Oversight of Intelligence Activities: The U.S. Experience: A Report*. Washington, D.C.: U.S. Government Printing Office, 1994.
- Lehninger, A.L., D.L. Nelson, and M.M. Cox. *Principles of Biochemistry*. 2nd ed. New York: Worth, 1993.
- Leitzel, Jim. *Economics and National Security*. Boulder, CO: Westview Press, 1993.
- Lentz, Harris M. *Assassins and Executions: An Encyclopedia of Political Violence, 1865-1986*. Jefferson, NC: McFarland, 1988.
- Leonard, Thomas M. *Panama, the Canal, and the United States: A Guide to Issues and References*. Claremont, CA: Regina Books, 1993.
- Lerner, K. Lee., and Brenda Wilmoth Lerner. *World of Genetics*. Detroit: Gale Group, 2001.
- Lerner, K. Lee., and Brenda Wilmoth Lerner. *World of Microbiology and Immunology*. Detroit: Gale Group, 2002.

- Lerner, K. Lee., and Brenda Wilmoth Lerner. *Encyclopedia of Science*, 3rd ed. Detroit: Gale Group, 2003.
- Lesser, Ian O. *Countering the New Terrorism*. Santa Monica, CA: RAND, 1999.
- Levine, Ira. *Quantum Chemistry*. 4th ed. New Jersey: Prentice Hall, 1991.
- Levine, Michael. *Deep Cover: The Inside Story of How DEA Infighting, Incompetence, and Subterfuge Lost Us the Biggest Battle of the Drug War*. New York: Delacorte Press, 1990.
- Levy, Steven. *Crypto: How the Code Rebels Beat the Government, Saving Privacy in the Digital Age*. New York: Viking, 2001.
- Lewis, Richard J., ed. *Hawley's Condensed Chemical Dictionary*. 13th ed. New York: Van Nostrand Reinhold, 1997.
- Libicki, Martin C. *What Is Information Warfare?* Washington, D.C.: National Defense University, 1995.
- Library of Congress. Congressional Research Service. *Soviet Intelligence and Security Services*. 2 vols. Washington, DC: GPO, 1972–1975.
- Lide, D. R., ed. *CRC Handbook of Chemistry and Physics*. Boca Raton: CRC Press, 2001.
- Lieven, Anatol. *Chechnya: Tombstone of Russian Power*. New Haven, CT: Yale University Press, 1998.
- Lifton, Robert Jay. *The Nazi Doctors: Medical Killing and the Psychology of Genocide*. New York: Basic Books, 1986.
- Lillesand, T.M., and R.W. Kiefer. *Remote Sensing and Image Interpretation*, 3rd ed. New York: John Wiley and Sons, Inc., 1994.
- Linacre, E., and B. Geerts. *Climates and Weather Explained*. New York: Routledge, 1997.
- Linde, Erik J. G. van de. *Quick Scan of Post 9/11 National Counterterrorism Policymaking and Implementation in Selected European Countries: Research Project for the Netherlands Ministry of Justice*. Santa Monica, CA: RAND Europe, 2002.
- Lindsey, Robert. *The Falcon and the Snowman: A True Story of Friendship and Espionage*. London: Jonathan Cape, 1980.
- Lisanti, Tom, and Louis Paul. *Film Fatales: Women in Espionage Films and Television, 1962–1973*. Jefferson, NC: McFarland, 2002.
- Livingston, M. Stanley, and John P. Blewett. *Particle Accelerators*. New York: McGraw-Hill, 1962.
- Local Law Enforcement Responds to Terrorism: Lessons in Prevention in Preparedness*. Washington, D.C.: Office of Community Oriented Policing Services, 2002.
- London, Barbara, and John Upton. *Photography*, Fifth ed. New York: Harper Collins College Publishers, 1994.
- Lord, Carnes. *The Presidency and the Management of National Security*. New York: Free Press, 1988.
- Lorenz, Edward N. *The Nature and Theory of the General Circulation of the Atmosphere*. Geneva: World Meteorological Organization, 1967.
- Lothes, Robert N., Michael B. Szymanski, and Richard G. Wiley. *Radar Vulnerability to Jamming*. Boston: Artech House, 1990.
- Louis, William Roger, and Roger Owen. *Suez 1956: The Crisis and Its Consequences*. New York: Oxford University Press, 1989.
- Lovell, Mary S. *Cast No Shadow: The Life of the American Spy Who Changed the Course of World War II*. New York: Pantheon Books, 1992.
- Lovett, James E. *Nuclear Materials: Accountability Management Safeguards*. American Nuclear Society, 1974.
- Lovins, Amory B., and L. Hunter Lovins. *Brittle Power: Energy Strategy for National Security*. Andover, MA: Brick House Publishing, 1982.
- Lovins, Amory B., and L. Hunter Lovins. *Energy/War: Breaking the Nuclear Link*. San Francisco: Friends of the Earth, 1980.
- Lowenthal, Mark M. *Intelligence: From Secrets to Policy*. Washington: Congressional Quarterly Press, 2000.
- Lowry, Edward D. *Interior Ballistics: How a Gun Converts Chemical Energy into Projectile Motion*. Garden City, NY: Doubleday, 1968.
- Loy, James, and Calvin B. Peters. *Understanding Behavior: What Primate Studies Tell Us about Human Behavior*. New York: Oxford University Press, 1991.
- Lubbe, J. C. A. van der. *Basic Methods of Cryptography*. New York: Cambridge University Press, 1995.
- Lutgens, Frederick K., Edward J. Tarbuck, and Dennis Tasa. *The Atmosphere: An Introduction to Meteorology*, 8th ed. New York: Prentice-Hall, 2000.
- Lykken, David T. *A Tremor in the Blood: Uses and Abuses of the Lie Detector*. Reading, Massachusetts: Perseus Books, 1998.
- Lynch, Charles T. *Practical Handbook of Materials Science*. Boca Raton, Florida: CRC Press, Inc., 1989.
- Macaulay, David, with Neil Ardley. *The New Way Things Work*. Boston: Houghton Mifflin, 1998.
- MacDonald, Elizabeth P. *Undercover Girl*. New York: Macmillan, 1947.
- MacEachin, Douglas J. *The Final Months of the War with Japan: Signals Intelligence, U.S. Invasion Planning, and the A-Bomb Decision*. Washington, D.C.: History Staff, Center for the Study of Intelligence, 1998.
- Madigan, M.M., J. Martinko, and J. Parker. *Brock Biology of Microorganisms*, 8th ed. Upper Saddle River: Prentice-Hall, 2000.
- Mahn, W. J. *Academic Laboratory Chemical Hazards Guidebook*. New York: Van Nostrand Rheinhold, 1991.
- Major, John. *Prize Possession: The United States and the Panama Canal, 1903–1979*. New York: Cambridge University Press, 1993.
- Malcolm, Noel. *Kosovo: A Short History*. New York: New York University Press, 1998.
- Mandelbaum, W. Adam. *The Psychic Battlefield: A History of the Military-Occult Complex*. New York: St. Martin's Press, 2000.
- Mandeles, Mark David. *The Development of the B-52 and Jet Propulsion: A Case Study in Organizational Innovation*. Maxwell Air Force Base, AL: Air University Press, 1998.
- Mandell, Douglas, et al. *Principles and Practice of Infectious Diseases*. New York: Churchill Livingstone, 1995.
- Mangano, Joseph, J. *Low level radiation and Immune System Damage: An Atomic Era Legacy*. Boca Raton: Lewis Publishers, 1998.
- Mangold, Tom. *Cold Warrior: James Jesus Angleton: The CIA's Master Spy Hunter*. New York: Simon and Schuster, 1991.

- Mann, Thomas E. *A Question of Balance: The President, Congress*. Washington, D.C.: Brookings Institution, 1990.
- Marchetti, Victor, and John Marks. *The CIA and the Cult of Intelligence*. New York: Alfred A. Knopf, 1974.
- Marenches, Count de Alexandre. *The Fourth World War: Diplomacy and Espionage in the Age of Terrorism*. New York: William Morrow and Company, 1992.
- Markvart, T., ed. *Solar Electricity*. Chichester, UK: John Wiley, 1994.
- Marples, David R., and Marilyn J. Young, eds. *Nuclear Energy and Security in the Former Soviet Union*. Boulder, Colo.: Westview, 1997.
- Marshall, Jonathan, Peter Dale Scott, and Jane Haapiseva-Hunter. *The Iran-Contra Connection: Secret Teams and Covert Operations in the Reagan Era*. Boston: South End Press, 1987.
- Martin, David C. *Wilderness of Mirrors*. New York: Harper & Row, 1980.
- Martin, Shannon E. *Bits, Bytes, and Big Brother: Federal Information Control in the Technological Age*. Westport, CT: Praeger, 1995.
- Martini, F. H., et al. *Fundamentals of Anatomy and Physiology*, 3rd edition. New Jersey: Prentice Hall, Inc., 1995.
- Matthews, Christopher K., and K. E. Van Holde, eds. *Biochemistry*. 2nd ed. New York: Benjamin/Cummings Publishing Company, 1966.
- Mauroni, Albert J. *America's Struggle with Chemical-Biological Warfare*. Westport, CN: Praeger Publishers, 2000.
- Mauskopf, Seymour H. *Chemical Sciences in the Modern World*. Pennsylvania: University of Pennsylvania Press, 1993.
- Mavis, Paul. *The Espionage Filmography: United States Releases, 1898 through 1999*. Jefferson, NC: McFarland, 2001.
- Mawson, Colin. *The Story of Radioactivity*. Englewood Cliffs, NJ: Prentice-Hall, 1969.
- Mayer, Kenneth R. *With the Stroke of a Pen: Executive Orders and Presidential Power*. Princeton, NJ: Princeton University Press, 2001.
- Mayer, Martin. *The Fed: The Inside Story of the How the World's Most Powerful Financial Institution Drives the Market*. New York: Free Press, 2001.
- McAllister, Therese, and Gene Corley. *World Trade Center Building Performance Study: Data Collection, Preliminary Observations, and Recommendations*. Washington, D.C.: Federal Emergency Management Agency, 2002.
- McAuliffe, Mary S. *Cuban Missile Crisis 1962*. Washington, D.C.: Center for the Study of Intelligence, 1992.
- McCarthy, Dennis V. N., with Philip W. Smith. *Protecting the President: The Inside Story of a Secret Service Agent*. New York: William Morrow, 1985.
- McCarthy, Shaun. *Intelligence Services for a Democratic South Africa: Ensuring Parliamentary Control*. London: Research for the Study of Conflict and Terrorism, 1996.
- McClintock, P. V. E., D. J. Meredith, and J. K. Wigmore. *Matter at Low Temperatures*. Glasgow: Blackie and Sons, 1984.
- McClure, Stuart, Joel Scambray, and George Kurtz. *Hacking Exposed: Network Security Secrets and Solutions, Fourth Edition*. Emeryville, CA: McGraw-Hill Osborne Media, 2003.
- McCormick, Anita Louise. *Shortwave Radio Listening for Beginners*. Blue Ridge Summit, PA: TAB Books, 1993.
- McCullough, John P., and Donald W. Scott, eds. *Experimental Thermodynamics*. New York: Plenum Press, 1968.
- McDougall, Walter. *The Heavens and the Earth: A Political History of the Space Race*. Baltimore: Johns Hopkins University Press, 1997.
- McIntosh, Elizabeth P. *Sisterhood of Spies: The Women of the OSS*. Annapolis, MD: Naval Institute Press, 1998.
- McKinley, James. *Assassination in America*. New York: Harper & Row, 1977.
- McMahon, Rober. *The Cold War on the Periphery*. New York, Columbia University Press 1994.
- McNeil, Ian. *An Encyclopaedia of the History of Technology*. New York: Routledge, 1996.
- McNeill, Robert. *Understanding the Weather*. Las Vegas: Arbor Publishers, 1991.
- Mearna, J., and W.C. Koller, eds. *Parkinson's Disease and Parkinsonism in the Elderly*. New York: Cambridge University Press, 2000.
- Medvedev, Zhores. *The Legacy of Chernobyl*. New York: W. W. Norton & Company, 1990.
- Melanson, Philip H. *The Politics of Protection: The U.S. Secret Service in the Terrorist Age*. New York: Praeger, 1984.
- Melton, H. Keith. *CIA Special Weapons and Equipment: Spy Devices of the Cold War*. New York: Sterling Publishing, 1993.
- Melton, H. Keith. *OSS Special Weapons and Equipment: Spy Devices of World War Two*. New York: Sterling Publishing, 1991.
- Melton, H. Keith. *The Ultimate Spy Book*. London & New York: Dorling Kindersley, Ltd., 1996.
- Mendez, A., and J. Mendez. *Spy Dust: Two Masters of Disguise Reveal the Tools and Operations That Helped Win the Cold War*. New York: Atria Books, 2002.
- Mendez, Antonio J. *The Master of Disguise: My Secret Life in the CIA*. New York: Morrow, 1999.
- Menges, Constantine Christopher. *Inside the National Security Council: The True Story of the Making and Unmaking of Reagan's Foreign Policy*. New York: Simon and Schuster, 1988.
- Merck Manual of Diagnosis and Therapy*, 17th edition. Edited by Mark H. Beers, and Robert Berkow. Whitehouse Station, NJ: Merck Research Laboratories, 1999.
- Meriam, J.L., and L.G. Kraige. *Engineering Mechanics, Dynamics*. 5th ed. New York: John Wiley & Sons, 2002.
- Mertz, L. *Recent Advances and Issues in Biology*. Phoenix, Arizona: Oryx Press, 2000.
- Merzbacher, E. *Quantum Mechanics*. New York: John Wiley & Sons, 1997.
- Meyer, Carl H., and Stephen M. Matyas. *Cryptography: A New Dimension in Computer Data Security*. New York: John Wiley & Sons 1982.
- Meyer, Cord. *Facing Reality: From World Federalism to the CIA*. New York: Harper & Row, 1980.
- Meyer, Henry Cord. *Airshipmen, Businessmen and Politics 1890-1940*. Washington DC: Smithsonian Institution Press, 1991.

- Meyer, Karl Ernest, and Shareen Blair Brysac. *Tournament of Shadows: The Great Game and the Race for Empire in Central Asia*. Washington, D.C.: Counterpoint, 1999.
- Meyers, Robert A. *Encyclopedia of Analytical Chemistry: Applications, Theory and Instrumentation*. New York: John Wiley & Sons, 2000.
- Meyers, Robert A., *Encyclopedia of Physics Science and Technology*. New York, NY: Academic Press, Inc., 1992.
- Michaels, Patrick J. *Sound and Fury: The Science and Politics of Global Warming*. Washington D. C.: Cato Institute, 1992.
- Michel, Lou and Dan Herbeck. *American Terrorist: Timothy McVeigh and the Oklahoma City Bombing*. New York: Regan Books, 2001.
- Micklos, David, A., and Greg A. Freyer. *DNA Science, A First Course in Recombinant DNA Technology*. United States: Cold Spring Harbor Laboratory Press and Carolina Biological Supply Company, 1990.
- Milano, James V. *Soldiers, Spies and the Rat Line: America's Undeclared War against the Soviets*. Washington: Brassey's, 1995.
- Miller, A. Ray. *The Cryptographic Mathematics of Enigma*. Ft. Meade, MD: National Security Agency, 2001.
- Miller, E. Willard, and Ruby Miller. *Environmental Hazards: Toxic Waste and Hazardous Material: A Reference Handbook*. Santa Barbara, Calif.: ABC-CLIO, 1991.
- Miller, Jay. *Lockheed Martin's Skunk Works*. North Branch, MN: Specialty Press, 1995.
- Miller, Nathan. *Spying for America: The Hidden History of U.S. Intelligence*. New York: Paragon House, 1989.
- Miller, Roger G. *To Save a City: The Berlin Airlift, 1948–1949*. Seattle, WA: University Press of the Pacific, 2002.
- Mitrokhin, Vasily, ed. *KGB Lexicon: The Soviet Intelligence Officer's Handbook*. London: Frank Cass, 2002.
- Mitrovich, Gregory. *Undermining the Kremlin: America's Strategy to Subvert the Soviet Bloc*. Ithaca, NY: Cornell, 2000.
- Mitton, Simon P., ed. *The Cambridge Encyclopedia of Astronomy*. Cambridge: Cambridge University Press, 1977.
- Modeling and Simulation: Linking Entertainment and Defense*. Washington, D.C.: National Academy Press, 1997.
- Mollin, Richard A. *An Introduction to Cryptography*. New York: Chapman & Hall, 2001.
- Money Factory*. Washington, D.C.: Bureau of Engraving and Printing, 1993.
- Montagu, Ewen. *Man Who Never Was*. London: Globe Pequot Press, 1997.
- Montague, Ludwell Lee. *General Walter Bedell Smith as Director of Central Intelligence*. University Park, PA: The Pennsylvania State University Press, 1992.
- Montplaisir, Jacques, and Roger Godbout, eds. *Sleep and Biological Rhythms: Basic Mechanisms and Applications to Psychiatry*. New York: Oxford University Press, 1990.
- Moore, David, and George McCabe. *Introduction to the Practice of Statistics*. New York: W. H. Freeman, 1989.
- Moore, Jim. *Very Special Agents: The Inside Story of America's Most Controversial Law Enforcement Agency—The Bureau of Alcohol, Tobacco, and Firearms*. Urbana: University of Illinois, 2001.
- Moore, John, and Nicholas D. Spencer. *Encyclopedia of Chemical Physics and Physical Chemistry*. Washington, D.C.: Institute of Physics, 2001.
- Moran, Joseph M., and Michael D. Morgan. *Essentials of Atmosphere and Weather*. New York: Macmillan Publishing Company, 1994.
- Morehouse, David. *Psychic Warrior: Inside the CIA's Stargate Program: The True Story of a Soldier's Espionage and Awakening*. New York: St. Martin's Press, 1996.
- Morgan, Ted. *A Covert Life: Jay Lovestone: Communist, Anti-Communist, and Spymaster*. New York: Random House, 1999.
- Moriarty, Laura J., and David L. Carter. *Criminal Justice Technology in the 21st Century*. Springfield, IL: Charles C. Thomas, 1998.
- Motto, Carmine J. *In Crime's Way: A Generation of U.S. Secret Service Adventures*. Boca Raton, FL: CRC Press, 2000.
- Mould, R. F. *Chernobyl Record: The Definitive History of the Chernobyl Catastrophe*. Bristol, England: Institute of Physics Publishing, 2000.
- Moyar, M. *Phoenix and the Birds of Prey: The CIA's Secret Campaign to Destroy the Viet Cong*. Annapolis, MD: Naval Institute Press, 1997.
- Mulhall, Douglas. *Our Molecular Future: How Nanotechnology, Robotics, Genetics, and Artificial Intelligence Will Change Our World*. Amherst, NY: Prometheus Books, 2002.
- Mulligan, Geoff. *Removing the Spam: Email Processing and Filtering*. Addison-Wesley, 1999.
- Munk W., P. Worcester, and C. Wunsch. *Ocean Acoustic Tomography*. Cambridge: Cambridge University Press, 1995.
- Munson, Bruce, et al. *Fundamentals of Mechanics*. 4th ed. New York: John Wiley and Sons, 2002.
- Murphy, Christine. *The Vaccine Dilemma*. New York: Lantern Books, 2000.
- Murphy, David E., Sergei A. Kondrashev, and George Bailey. *Battleground Berlin: CIA vs. KGB in the Cold War*. New Haven, CT: Yale University Press, 1997.
- Murphy, Douglas, B. *Fundamentals of Light Microscopy and Electronic Imaging*. New York: Wiley-Liss, 2001.
- Murray, John, James H. Murray, and Barnet Resnick. *A Guide to Taser Technology: Stunguns, Lies, and Videotape*. Dana Point: Whitewater Press, 1997.
- Murray, Raymond L. *Nuclear Energy*. 3rd ed. New York: Pergamon Press, 1988.
- Murray, Williamson, and Allan Reed Millett. *Military Innovation in the Interwar Period*. New York: Cambridge University Press, 1996.
- Musciano, Walter A. *Warbirds of the Sea: A History of Aircraft Carriers and Carrier-Based Aircraft*. Atglen, PA: Schiffer Publishing, 1994.
- Musicant, Ivan. *The Banana Wars: A History of United States Military Intervention in Latin America from the Spanish-American War to the Invasion of Panama*. New York: Macmillan, 1990.

- Myroie, Laurie. *Study of Revenge: The First World Trade Center Attack and Saddam Hussein's War Against America*. Washington, D.C.: AEI Press, 2001.
- Nanavati, Samir, Michael Thieme, and Raj. Nanavati. *Biometrics: Identity Verification in a Networked World*. New York: Wiley and Sons, 2002.
- Nataro, J.P., M.J. Blaser, and S. Cunningham-Rundles. *Persistent Bacterial Infections*. Washington: American Society for Microbiology, 2000.
- Nathan, James. *Anatomy of the Cuban Missile Crisis*. Westport, CT: Greenwood Press, 2001.
- National Academy of Sciences. *Veterans and Agent Orange: Health Effects of Herbicides Used in Vietnam*. Washington, DC: National Academy Press, 1994.
- National Communications System for Emergency Response Personnel*. Washington, D.C.: Government Printing Office, 2001.
- National Communications System, 1963–1998: 35th Anniversary*. Arlington, VA: National Communications System, 1998.
- National Infrastructure Protection Center (NIPC): A Public-Private Partnership to Protect America's Critical Infrastructures*. Washington, D.C.: U.S. Department of Justice, 2002.
- National Research Council, Computer Science and Telecommunications Board. *Cyber Security Today and Tomorrow: Pay Now or Pay Later*. Washington, DC: The National Academies Press, 2002.
- National Security: The Use of Presidential Directives to Make and Implement United States Policy: Report to the Chairman, Committee on Government Operations, House of Representatives*. Washington, D.C.: Government Printing Office, 1988.
- National Transportation Strategic Research Plan*. Washington, D.C.: National Science and Technology Council, 2000.
- Naval Criminal Investigative Service: To Protect and Serve*. Washington, D.C.: U.S. Department of the Navy, 1994.
- Navarra, John G. *Atmosphere, Weather and Climate*. Philadelphia: W.B. Saunders Co., 1979.
- Naveh, Ben-Zin and Azrid Lorber, eds. *Theater Ballistic Missile Defense*. Reston, VA: American Institute of Aeronautics and Astronautics, 2001.
- Naylor, R.T. *Wages of Crime: Black Markets, Illegal Finance, and the Underworld Economy*. Ithaca, NY: Cornell University, 2002.
- Nelson, K.E., C.M. Williams, and N.M.H. Graham. *Infectious Disease Epidemiology: Theory and Practice*. Gaithersburg: Aspen Publishers, 2001.
- Nelson, Robert A. *SI: The International System of Units*. Stony Brook, N.Y.: American Association of Physics Teachers, 1982.
- Neustaedter, Randall. *The Vaccine Guide: Risks and Benefits for Children and Adults*. Berkeley: North Atlantic Books, 2002.
- Newman, Elizabeth L. *Security Clearance Law and Procedure*. Arlington, VA: Dewey Publications, 1998.
- Newton, David E. *Encyclopedia of Cryptology*. Santa Barbara, CA: ABC-CLIO, 1997.
- Newton, David E. *Particle Accelerators: From the Cyclotron to the Superconducting Super Collider*. New York: Franklin Watts, 1989.
- Nickell, Joe, and John F. Fischer. *Crime Science: Methods of Forensic Detection*. Lexington: University Press of Kentucky, 1999.
- Nieto, Marcus, Kimberly Johnston-Dodds, and Charlene Simmons. *Public and Private Applications of Video Surveillance and Biometric Technologies*. Sacramento, CA: California Research Bureau, California Public Library, 2002.
- Noor, Ahmed Khairy, and Samuel L. Venneri. *Future Aeronautical and Space Systems*. Reston, VA: American Institute of Aeronautics and Astronautics, 1997.
- Notton, John. "The Use of Technology in Policing the City of London," in proceedings from the *International Carnahan Conference on Security Technology*, Larry D. Sanson, ed. 1998.
- Nuclear Power, Nuclear Fuel Cycle and Waste Management, Part C: Status and Trends, 1993*. Lanham, MD: UNIPUB, 1993.
- Nuclear Safety: The Defense Nuclear Facilities Safety Board's First Year of Operation: Report to Congressional Requesters*. Washington, D.C.: General Accounting Office, 1991.
- Nussbaum, R. L., R. R. McInnes, and H. F. Willard. *Thompson and Thompson Genetics in Medicine, Sixth Edition*. Philadelphia, PA: Saunders, 2001.
- Nutter, John Jacob. *The CIA's Black Ops: Covert Action, Foreign Policy, and Democracy*. Amherst, NY: Prometheus Books, 2000.
- Ojeda, Auriana. *Drug Trafficking*. San Diego, CA: Greenhaven Press, 2002.
- Olah, George A., ed. *Chemistry of Energetic Materials*. San Diego: Academic Press, 1991.
- Olin, Harold B. *Construction; Principles, Materials and Methods*. Danville, Ill.: Interstate Printers and Publishers, 1980.
- Olmstead, A. T. *History of the Persian Empire and the Ancient MidEast*. Chicago: University of Chicago Press, 1959.
- One Nation: America Remembers September 11, 2001*. Boston: Little, Brown, 2001.
- O'Neil, Maryadele J. *Merck Index: An Encyclopedia of Chemicals, Drugs, & Biologicals*. 13th ed. Whitehouse Station, NJ: Merck & Co., 2001.
- Operation DISA: A Continuing Evolution*. Arlington, VA: Defense Information Systems Agency, 1996.
- Optical Document Security*. Boston: Artech House, 1998.
- Orphan, R. C. *A Study of Applying the Atmospheric Release Advisory Capability to Nuclear Power Plants*. Springfield, VA: Department of Energy, 1978.
- Osborn, Shane, and Malcolm McConnell. *Born to Fly: The Untold Story of the Downed American Reconnaissance Plane*. New York: Broadway Books, 2001.
- Ostmann, Robert. *Acid Rain: A Plague Upon the Waters*. Minneapolis: Dillon, 1982.
- Ostrander, Sheila, and Lynn Schroeder. *Psychic Discoveries Behind the Iron Curtain*. Englewood Cliffs, NJ: Prentice-Hall, 1970.
- O'Toole, G. J. A. *Honorable Treachery: A History of Intelligence, Espionage, and Covert Action from the American Revolution to the CIA*. New York: Atlantic Monthly Press, 1991.
- O'Toole, G. J. A. *The Encyclopedia of American Intelligence and Espionage*. New York: Facts on File, 1988.



- Ottis, Sherri Greene. *Silent Heroes: Downed Airmen and the French Underground*. Lexington, KY: University of Kentucky Press, 2001.
- Ousby, Ian. *Occupation*. Lanham, MD: Cooper Square Press, 2000.
- Owen, David. *Hidden Secrets*. Buffalo, NY: Firefly Books, 2002.
- Pace, Steve. *Lockheed Skunk Works*. Osceola, WI: Motorbooks International, 1992.
- Packard, Wyman H. *A Century of U.S. Naval Intelligence*. Washington, D.C.: Naval Historical Center, 1996.
- Pagana, K.D., *Mosby's Manual of Diagnostic and Laboratory Tests*. St. Louis: Mosby, Inc., 1998.
- Paglin, Max D., editor. *A Legislative History of the Communications Act of 1934*. New York: Oxford University Press, 1990.
- Park, William. *Defending the West: A History of NATO*. Brighton: Wheatsheaf, 1986.
- Parker, James E. *Codename Mule: Fighting the Secret War in Laos for the CIA*. Annapolis, MD: Naval Institute Press, 1995.
- Parrish, Michael. *Soviet Security and Intelligence Organizations, 1917–1990: A Biographical Dictionary and Review of Literature in English*. Westport, CT: Greenwood, 1991.
- Parrish, Michael. *The Lesser Terror: Soviet State Security, 1939–1953*. Westport, CT: Praeger, 1996.
- Patrick, Dale R. and Stephen W. Fardo. *Understanding Electricity and Electronics*. Upper Saddle River, NJ: Prentice Hall, 1989.
- Pedlow G.W., and Welzenbach, D.E. *The CIA and the U-2 Program*. Washington, D.C.: History Staff, Center for the Study of Intelligence, 1998.
- Peebles, Curtis. *The CORONA Project*. Annapolis: Naval Institute Press, 1997.
- Peebles, Curtis. *Shadow Flights: America's Secret Air War Against the Soviet Union*. Novato, CA: Presidio, 2000.
- Peebles, Curtis. *The Moby Dick Project: Reconnaissance Balloons over Russia*. Washington, D.C.: Smithsonian Institution Press, 1991.
- Peierls, R. E. *Atomic History*. New York: Springer-Verlag, 1997.
- Permissible Dose: A History of Radiation Protection in the Twentieth Century*. Berkeley: University of California Press, 2000.
- Persico, Joseph E. *Casey: From the OSS to the CIA*. New York: Viking Penguin, 1990.
- Persico, Joseph E. *Roosevelt's Secret War: FDR and World War II Espionage*. New York: Random House, 2001.
- Petersen, Julie K. *Understanding Surveillance Technologies: Spy Devices, their Origins & Applications*. Boca Raton, FL : CRC Press, 2001.
- Peterson, M. N. A. *Initial Reports of the Deep Sea Drilling Project II*. Washington: Government Printing Office, 1970.
- Petit, Michael. *Peacekeepers at War: A Marine's Account of the Beirut Catastrophe*. Boston: Faber and Faber, 1986.
- Pforzheimer, Walter, ed. *Bibliography of Intelligence Literature: A Critical and Annotated Bibliography of Open-Source Intelligence Literature*. 8th ed. Washington, DC: Defense Intelligence College, 1985.
- Phillips, Bill. *The Complete Book of Locks and Locksmithing*. New York: McGraw-Hill, 1995.
- Phillips, David Atlee. *The Night Watch: 25 Years of Peculiar Service*. New York: Atheneum, 1977.
- Phillips, David Atlee. *Careers in Secret Operations: How to Be a Federal Intelligence Officer*. Frederick, MD: University Publications of America, 1984.
- Physicians Desk Reference 2003 with Physicians Desk Reference Family Guide*. Montvale, NJ: Medical Economics, 2002.
- Pincher, Chapman. *The Secret Offensive*. New York: St. Martin's, 1985.
- Pincher, Chapman. *The Spycatcher Affair*. New York: St. Martin's Press, 1988.
- Pinck, D.C., G.M.T. Jones, and C.T. Pinck. *Stalking the History of the Office of Strategic Services: An OSS Bibliography*. Boston: The OSS/Donovan Press, 2000.
- Piresein, Robert William. *The Voice of America: A History of the International Broadcasting Activities of the United States Government, 1940–1962*. New York: Arno Press, 1979.
- Plischke, Elmer. *U.S. Department of State: A Reference History*. Westport, CT: Greenwood Press, 1999.
- Pocock, Chris. *Dragon Lady: The History of the U-2 Spyplane*. Shrewsbury, UK: Airline Publishing, 1989.
- Politkovskaia, Anna. *A Dirty War: A Russian Reporter in Chechnya*. London: Harvill, 2001.
- Pollock, David A. *Methods of Electronic Audio Surveillance*. Springfield, IL: Thomas, 1973.
- Polmar, Norman. *The Naval Institute Guide to the Ships and Aircraft of the U.S. Fleet*. Annapolis, MD: Naval Institute Press, 1993.
- Polmar, Norman, and Thomas B. Allen. *Spy Book: The Encyclopedia of Espionage*. New York: Random House, 1997.
- Poolos, J. *Nerve Gas Attack on the Tokyo Subway*. Rosen Publishing Group Inc., 2002.
- Porch, Douglas. *The French Secret Services: From the Dreyfus Affair to the Gulf War*. New York: Farrar, Straus & Giroux, 1995.
- Porter, Roy, and Marilyn Ogilvie, consultant editors. *The Biographical Dictionary of Scientists*. New York: Oxford University Press, 2000.
- Porter, Ted, and Dorothy Ross, eds. *The Cambridge History of Science: Volume 7, The Modern Social Sciences*. Cambridge: Cambridge University Press, 2003.
- Pottier, John. *Anthropology of Food: The Social Dynamics of Food Security*. Oxford: Polity Press, 1999.
- Powell, Colin L., and Joseph E. Persico. *My American Journey*. New York: Ballantine Books, 1996.
- Power, Samantha. *A Problem from Hell: America in the Age of Genocide*. New York: Basic Books, 2002.
- Powers, Thomas. *The Man Who Kept the Secrets: Richard Helms and the CIA*. New York: Alfred A. Knopf, 1979.
- Prados, John. *Combined Fleet Decoded: The Secret History of American Intelligence and the Japanese Navy in World War II*. New York: Random House, 1995.
- Prados, John. *Keepers of the Keys: A History of the National Security Council from Truman to Bush*. New York: William Morrow & Company, Inc., 1991.

- Prados, John. *Lost Crusader: The Secret Wars of CIA Director William Colby*. New York: Oxford University Press, 2003.
- Prados, John. *Presidents' Secret Wars: CIA and Pentagon Covert Operations from World War II through Iranscam*. New York: William Morrow, Co., 1986.
- Prados, John. *The Soviet Estimate: U.S. Intelligence Analysis and Russian Military Strength*. New York: Dial Press, 1982.
- Prange, Gordon W. *At Dawn We Slept: The Untold Story of Pearl Harbor*. New York: McGraw-Hill, 1981.
- Prescott, L., J. Harley, and D. Klein. *Microbiology* 5th ed. New York: McGraw-Hill, 2002.
- Press, Frank and Raymond Siever. *Understanding Earth*. New York: W. H. Freeman and Company, 2000.
- Preston, Anthony. *Carriers*. New York: Gallery Books, 1993.
- Preston, Edmund. *FAA Historical Chronology: Civil Aviation and the Federal Government, 1926–1996*. Washington: DOT/FAA, 1998.
- Preston, R. *The Demon in the Freezer*. New York: Random House, 2002.
- Preston, Richard. *The Demon in the Freezer: A True Story*. New York: Random House, 2002.
- Price, Alfred. *War in the Fourth Dimension: U.S. Electronic Warfare, from the Vietnam War to the Present*. London: Greenhill, 2001.
- Primrose, S.P. *Principles of Genome Analysis*. Oxford: Blackwell, 1995.
- Principal Officers of the Department of State and United States Chiefs of Mission, 1778–1990*. Washington, D.C.: U.S. Department of State, 1991.
- Pritchard, Michael, and Douglas St. Denny. *Spy Camera: A Century of Detective and Subminiature Cameras*. London: Classic Collections, 1993.
- Proakis, John G. *Digital Communications*. New York: McGraw-Hill, 2001.
- Purcell, William P. "Benzene." *Kirk-Othmer Encyclopedia of Chemical Technology*. 4th ed. Suppl. New York: John Wiley & Sons, 1998.
- Rabilloud, Thierry. *Proteome Research: Two-Dimensional Gel Electrophoresis and Identification Methods (Principles and Practice)*. Berlin: Springer Verlag, 2000.
- Ranelagh, John. *The Agency: The Rise and Decline of the CIA*. New York: Simon & Schuster, 1987.
- Record, Jeffrey. *Making War, Thinking History: Munich, Vietnam, and Presidential Uses of Force from Korea to Kosovo*. Annapolis, MD: Naval Institute Press, 2002.
- Reeve, Simon. *The New Jackals: Ramzi Yousef, Osama bin Laden, and the Future of Terrorism*. Boston: Northeastern University Press, 1999.
- Rehnquist, William H. *All the Laws But One: Civil Liberties in Wartime*. New York: Alfred A. Knopf, 1998.
- Reisman, W. Michael, and James E. Baker. *Regulating Covert Action: Practices, Contexts, and Policies of Covert Coercion Abroad in International and American Law*. New Haven, CT: Yale University Press, 1992.
- Reist, Parker C. *Introduction to Aerosol Science*. New York: Macmillan, 1989.
- Rhodes, Richard. *Dark Sun: The Making of the Hydrogen Bomb (Sloan Technology Series)*. Simon & Schuster, 1995.
- Rich, Ben and Leo Janos. *Skunk Works*. New York: Bantam, 1994.
- Richelson, Jeffrey T. *A Century of Spies: Intelligence in the Twentieth Century*. New York: Oxford University Press, 1995.
- Richelson, Jeffrey T. *The U.S. Intelligence Community*, fourth edition. Boulder, CO: Westview Press, 1999.
- Richelson, Jeffrey T. *The Wizards of Langley*. Boulder, Colo.: Westview, 2001.
- Richelson, Jeffrey. *The Ties That Bind: Intelligence Cooperation Between the UKUSA Countries*. Boston: Unwin Hyman, 1990.
- Richman, D. D., and R. J. Whitley. *Clinical Virology*. 2nd ed. Washington: American Society for Microbiology, 2002.
- Ridgway, Matthew B. *The Korean War: How We Met the Challenge; How All-Out Asian War Was Averted; Why MacArthur Was Dismissed; Why Today's War Objectives Must Be Limited*. Garden City, NY: Doubleday, 1967.
- Riebling, Mark. *Wedge: The Secret War Between the FBI and CIA*. New York: Alfred A. Knopf, 1994.
- Rifkin, J. *The Biotech Century*. Putnam Publishing Group, 1998.
- Rihaczek, August W., and Stephen J. Hershkowitz. *Theory and Practice of Radar Target Identification*. Boston: Artech House, 2000.
- Riley, Kevin Jack, and Bruce Hoffman. *Domestic Terrorism: A National Assessment of State and Local Preparedness*. Santa Monica, CA: RAND Corporation, 1995.
- Riley, Kevin Jack. *Crack, Powder Cocaine, and Heroin: Drug Purchase and Use Patterns in Six U.S. Cities*. Washington, D.C.: National Institute of Justice, 1998.
- Rimoin, David L. *Emery and Rimoin's Principles and Practice of Medical Genetics*. London; New York: Churchill Livingstone, 2002.
- Ripley, Randall B., and James M. Lindsay. *U.S. Foreign Policy After the Cold War*. Pittsburgh: University of Pittsburgh Press, 1997.
- Rivers, Gayle, and James Hudson. *The Teheran Contract*. Garden City: New York: Doubleday & Company, 1981.
- Robarge, David. *Intelligence in the War for Independence*. Washington, D.C.: Center for the Study of Intelligence, 1997.
- Roberts, Brad. *Biological Weapons: Weapons of the Future?* Washington, D.C.: Center for Strategic and International Studies, 1993.
- Roberts, Brad. *U.S. Foreign Policy After the Cold War*. Cambridge, MA: MIT Press, 1992.
- Robertson, Kenneth G. "The Study of Intelligence in the United States." *Comparing Foreign Intelligence: The U.S., the USSR, the U.K. & the Third World*. R. Godson, ed. Washington, DC: Pergamon-Brassey's, 1988.
- Rocca, Raymond G., and John J. Dziak. *Bibliography on Soviet Intelligence and Security Services*. Boulder, CO: Westview, 1985.
- Rogers, Paul. *Political Violence and Asymmetric Warfare*. (U.S.-European Forum Paper) Washington: Brookings Institution, 2001.
- Roit, I.M. *Roit's Essential Immunology*. Oxford: Blackwell Science Ltd., 1997.

- Rolleff, Tamara. ed. *The Atom Bomb*. San Diego, CA: Greenhaven Press, 2000.
- Roosevelt, Archibald. *For Lust of Knowing: Memoirs of an Intelligence Officer*. Boston: Little, Brown, 1988.
- Roosevelt, Kermit. *Countercoup: The Struggle for the Control of Iran*. New York: McGraw-Hill Book Co., 1979.
- Rose, N.R. *Manual of Clinical Laboratory Immunology*, 4th ed. Washington: American Society for Microbiology, 2002.
- Rose, P.K. *Black Dispatches: Black American Contributions to Union Intelligence during the Civil War*. Washington, D.C.: Center for Study of Intelligence, 1999.
- Rosen, Jeffrey. *The Unwanted Gaze: The Destruction of Privacy in America*. New York: Random House, 2000.
- Rosen, Kenneth H., and John G. Michaels. *Handbook of Discrete and Combinatorial Mathematics*. Boca Raton, FL: CRC Press 2000.
- Rositzke, Harry A. *CIA's Secret Operations: Espionage, Counterespionage, and Covert Action*. Boulder, CO: Westview Press, 1988.
- Ross, David F., and J. Don Read. *Adult Eyewitness Testimony: Current Trends and Developments*. New York: Press Syndicate of the University of Cambridge, 1994.
- Rossiter, Margaret. *Women in the Resistance*. New York: Praeger, 1991.
- Roukis, George S., and Hugh Conway. *Global Corporate Intelligence: Opportunities, Technologies, and Threats in the 1990s*. New York: Quorum Books, 1990.
- Rudgers, David F. *Creating the Secret State: The Origins of the Central Intelligence Agency*. Lawrence, KS: University of Kansas Press, 2000.
- Rudman, Warren B. *Science at Its Best, Security at Its Worst: A Report on Security Problems at the U.S. Department of Energy*. Washington, D.C.: President's Foreign Intelligence Advisory Board, 1999.
- Ruffner, Kevin. ed. *CORONA: America's First Satellite Program*. Washington, D.C.: CIA History Staff, 1995.
- Ryan, Charles W. *Basic Electricity: A Self-Teaching Guide*. 2nd ed. New York: John Wiley & Sons, Inc., 1986.
- Ryan, Ray and Lisa A. Doyle. *Basic Digital Electronics*, 2nd ed. Blue Ridge Summit, PA: Tab Books, 1990.
- Sabins, F.S., Jr. *Remote Sensing Principles and Interpretation*. 2nd ed. New York: W.H. Freeman and Company, 1987.
- Saferstein, Richard. *Criminalistics: An Introduction to Forensic Science*. Upper Saddle River, NJ: Prentice Hall, 1998.
- Sagan, Scott D., and Kenneth N. Waltz. *The Spread of Nuclear Weapons: A Debate Renewed*, Second Edition. New York: W. W. Norton & Co., 2003.
- Sage, Kingsley, and Stewart Young. "Computer Vision for Security Applications," in proceedings from the *International Carnahan Conference on Security Technology*, Larry D. Sanson, ed. 1998.
- Sakharov, Vladimir. *High Treason*. New York: Ballentine Books, 1981.
- Salyers, Abigail, A., and Dixie D. Whitt. *Bacterial Pathogenesis: A Molecular Approach*. Washington, D.C.: American Society for Microbiology Press, 2001.
- Sam Adams. *War of Numbers: An Intelligence Memoir*. South Royalton, Vermont: Steerforth Press, 1994.
- Sayers, Michael, and Albert Eugene Kahn. *Sabotage! The Secret War against America*. New York: Harper & Brothers, 1942.
- Scanlon, Charles Francis. *In Defense of the Nation: DIA at Forty Years*. Washington, D.C.: Defense Intelligence Agency, 2002.
- Schecter J., and L.J. Schecter. *Sacred Secrets: How Soviet Intelligence Operations Changed American History*. Washington, D.C.: Brassey's, 2002.
- Schleher, D. Curtis. *Electronic Warfare in the Information Age*. Boston: Artech House, 1999.
- Schlesinger, S., S. Kinzer. *Bitter Fruit: The Untold Story of the American Coup in Guatemala*. New York: Doubleday, 1982.
- Schlessinger, Monroe. *Infrared Technology Fundamentals*. New York: Marcel Dekker, 1995.
- Schmidt, Gustav, ed. *A History of NATO: The First Fifty Years*. New York: Palgrave, 2001.
- Schneier, Bruce. *Secrets and Lies: Digital Security in a Networked World*. New York: John Wiley, 2000.
- Schobert, Harold H. *The Chemistry of Hydrocarbon Fuels*. Boston: Butterworth's, 1990.
- Schrecker, Ellen. *Many Are the Crimes: McCarthyism in America*. Boston: Little, Brown and Company, 1998.
- Schuck, P.H.H. *Agent Orange on Trial: Mass Toxic Disasters in the Courts*. Boston: Harvard University Press, 1990.
- Schwartz, Winn. *Cybershock: Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorists, and Weapons of Mass Disruption*. New York: Thunder's Mouth Press, 2000.
- Schwartz, Winn. *Information Warfare: Chaos on the Electronic Superhighway*. New York: Thunder's Mouth Press, 1994.
- Scientific Assessment of Ozone Depletion*. vols. I and II. World Meteorological Organization Global Ozone Research and Monitoring Project, 1988.
- Scientists and Engineers: Directorate for Scientific and Technical Intelligence, Directorate for Foreign Intelligence*. Washington, D.C.: Defense Intelligence Agency, 1987.
- Scriver, Charles R., et al. *The Metabolic and Molecular Bases of Inherited Disease*, 8th ed. New York: McGraw-Hill Professional Book Group, 2001.
- Seagrave, Sterling. *Yellow Rain: A Journey Through the Terror of Chemical Warfare*. New York: M. Evans and Company, 1981.
- Sebag-Montefiore, Hugh. *Enigma: The Battle for the Code*. New York: John Wiley & Sons, 2001.
- Seberry, J. and J. Pieprzyk. *Cryptography: An Introduction to Computer Security*. New York: Prentice Hall, 1989.
- Settles, Gary S. *Schlieren and Shadowgraph Techniques*. Heidelberg: Springer-Verlag, 2001.
- Sexton, Donal J. *Signals Intelligence in World War II: A Research Guide*. Westport, CT: Greenwood Press, 1996.
- Shannon, Michel L. *Bug Book: Everything You Ever Wanted to Know About Electronic Eavesdropping...But Were Afraid to Ask*. Boulder: Paladin Press, 2000.
- Shaw, John M. "Jet Engines." *Magill's Survey of Science: Applied Science Series*. Edited by Frank N. McGill. Pasadena, CA: Salem Press, 1993.

- Sherick, L. G. *How to Use the Freedom of Information Act (FOIA)*. New York: Arco, 1978.
- Sherman, Chris, and Gary Price. *The Invisible Web: Uncovering Information Sources Search Engines Can't See*. Medford, NJ: CyberAge Books, 2001.
- Shevchenko, Arkady N. *Breaking with Moscow*. New York: Alfred A. Knopf, 1985.
- Shnayerson, Michael, and Mark J. Plotkin. *The Killers Within: The Deadly Rise of Drug Resistant Bacteria*. New York: Little Brown & Company, 2002.
- Shubert, Hiltmar, Andre Kuznetsov, and Audrey Kuznetsov. *Detection of Explosives and Landmines*. Hingham, MA: Kluwer Academic Publishers, 2002.
- Shulman, Holly Cowan. *The Voice of America: Propaganda and Democracy, 1941–1945*. Madison: The University of Wisconsin Press, 1990.
- Shulsky, Abram N. *Silent Warfare*. Washington, D.C.: Brassey's, 1991.
- Shultz, Richard G. *The Secret War Against Hanoi: Kennedy's and Johnson's Use of Spies, Saboteurs, and Covert Warriors in North Vietnam*. New York: HarperCollins, 1999.
- Sick, Gary. *All Fall Down: America's Tragic Encounter with Iran*. New York: Random House, 1985.
- Sicker, Martin. *The Geopolitics of Security in the Americas: Hemispheric Denial from Monroe to Clinton*. Westport, CT: Praeger, 2002.
- Siegel, J. P., and R. T. Finley. *Women in the Scientific Search*. Scarecrow, 1985.
- Sifakis, Carl. *Encyclopedia of Assassinations*. New York: Facts on File, 1991.
- Sifton, David W., editor. *PDR Guide to Biological and Chemical Warfare Response*. Montvale, NJ: Thompson/Physician's Desk Reference, 2002.
- Siljander, Raymond P. *Applied Surveillance Photography*. Springfield, IL: Thomas, 1975.
- Simon, Jeffrey D. *The Terrorist Trap: America's Experience with Terrorism*. Bloomington and Indianapolis: Indiana University Press, 1994.
- Sincerbox, Glenn T. *Counterfeit Deterrent Features for the Next-Generation Currency Design*. Washington, D.C.: National Academy Press, 1993.
- Singer, M. and P. Berg. *Genes and Genomes*. Mill Valley, CA: University Science Books, 1991.
- Singh, Simon. *The Code Book: The Evolution of Secrecy from Mary, Queen of Scots to Quantum Cryptography*. New York: Doubleday, 1999.
- Sittig, M. *Handbook of Toxic and Hazardous Chemicals and Carcinogens*. 3rd ed. Park Ridge, NJ: Noyes Publications, 1991.
- Sivard, R. L. *World Military and Social Expenditures, 1993*. World Priorities, 1993.
- Sklar, Lawrence. *Philosophy of Physics*. Boulder, CO: Westview Press, 1992.
- Skolnik, Merrill I. *Introduction to RADAR Systems*. New York: McGraw Hill, 2001.
- Slater, J.C. *Introduction to Chemical Physics*. New York: Dover Publications, Inc., 1939.
- Slayter, Elizabeth, and Henry Slater. *Light and Electron Microscopy*. Cambridge: Cambridge University Press, 1992.
- Slichter, Charles P. *Principles of Magnetic Resonance*. New York: Harper Row, 1963.
- Sloane, Eugene A. *The Complete Book of Locks, Keys, Burglar and Smoke Alarms, and Other Security Devices*. New York: Morrow, 1977.
- Smist, Frank John. *Congress Oversees the United States Intelligence Community, 1947–1989*. Knoxville: University of Tennessee Press, 1990.
- Smith, A.D., et al. *Oxford Dictionary of Biochemistry and Molecular Biology*. New York: Oxford University Press, 1997.
- Smith, Charles O. *The Science of Engineering Materials*. Englewood Cliffs, NJ: Prentice-Hall, 1969.
- Smith, Dennis. *Report from Ground Zero: The Story of the Rescue Efforts at the World Trade Center*. New York: Viking, 2002.
- Smith, Edward E., and R. Lednicky. *The Okhrana: The Russian Department of Police—A Bibliography*. Stanford, CA: Hoover Institution, 1967.
- Smith, G. Davidson. *Combating Terrorism*. New York: Routledge, 1990.
- Smith, H. C. *The Illustrated Guide to Aerodynamics*. Blue Ridge Summit, PA: Tab Books, 1992.
- Smith, H., C.J. Dornan, G. Dougan, et al. (eds.). *The Activities of Bacterial Pathogens In Vivo*. River Edge, NJ: World Scientific, 2001.
- Smith, Michael. *Station X: The Codebreakers of Bletchley Park*. London: Channel 4 Books, 2000.
- Smith, Michael. *Station X: Decoding Nazi Secrets*. London: TV Books 2000.
- Smith, Myron J., Jr. *Cloak-and-Dagger Bibliography*. Metuchen, NJ: Scarecrow Press, 1976.
- Smith, R. P. *A Primer of Environmental Toxicology*. Philadelphia: Lea & Febiger, 1992.
- Snider, Britt. *Sharing Secrets with Lawmakers: Congress as a User of Intelligence*. Washington, D.C.: CIA History Staff, Center for the Study of Intelligence, 1997.
- Solomons, T.W. Graham. *Fundamentals of Organic Chemistry*. 5th ed. New York: John Wiley & Sons, Inc., 1997.
- Sontag, Sherry. *Blind Man's Bluff: The Untold Story of American Submarine Espionage*. New York: Public Affairs, 1998.
- Sorley, Lewis. *A Better War: The Unexamined Victories and Final Tragedy of America's Last Years in Vietnam*. New York: Harcourt Brace, 1999.
- Sparrow, Elizabeth. *Secret Service: British Agents in France, 1792–1815*. Woodbridge, UK: Boydell Press, 1999.
- Spignesi, Stephen J. *In the Crosshairs: Famous Assassinations and Attempts*. New York: New Page Books, 2003.
- Spitzner, Lance. *Honeypots: Tracking Hackers*. Boston: Addison Wesley Professional, 2002.
- Sproule, J. Michael. *Channels of Propaganda*. Bloomington: EDINFO Press, 1994.
- Stallings, William. *Cryptography and Network Security: Principles and Practice*, 3rd. ed. Upper Saddle River, NJ: Prentice Hall, 2002.

- Stanier, R.Y., J.L. Ingraham, M.L. Wheelis, and P.R. Painter. *General Microbiology*, 5th ed. U.K.: Macmillan Press Ltd., 1993.
- Stanley, Roy M. *World War II Photo Intelligence*. New York: Scribner, 1981.
- Stanley, Zell. *An Annotated Bibliography of the Open Literature on Deception*. Santa Monica, CA: RAND, 1985.
- Starnes, John. *Closely Guarded: A Life in Canadian Security and Intelligence*. Toronto: University of Toronto Press, 2001.
- State 2000: *A New Model for Managing Foreign Affairs: Report of the U.S. Department of State Management Task Force*. Washington, D.C.: U.S. Government Printing Office, 1993.
- Steede-Terry, K. *Integrating GIS and the Global Positioning System*. ESRI Press, 2000.
- Stephens, Frederick John, and Michael Boxall. *Fighting Knives: An Illustrated Guide to Fighting Knives and Military Survival Weapons of the World*. New York: Arco, 1980.
- Stephenson, Michael, and Roger Hearn. *The Nuclear Casebook*. London: Frederick Muller Limited, 1983.
- Sterling, D. *Technician's Guide to Fiber Optics (AMP)*. Albany, NY: Delmar Publishers Inc., 1987.
- Stern, Philip Van Doren. *Secret Missions of the Civil War*. Wings Books, New York/Avenel, NJ, 1990.
- Steury, Donald P. ed. *Intentions and Capabilities: Estimates on Soviet Strategic Forces*. Washington, D.C.: History Staff, Center for the Study of Intelligence, 1996.
- Steury, Donald P. ed. *On the Front Lines of the Cold War: Documents on the Intelligence War in Berlin*, Washington, D.C.: CIA History Staff, Center for the Study of Intelligence, 1999.
- Stiglitz, Joseph E. *Globalization and its Discontents*. New York: W.W. Norton & Co., 2002.
- Stinson, Douglas R. *Cryptography: Theory and Practice*. New York: Chapman & Hall, 2002.
- Stocchi, E. *Industrial Chemistry*, vol. 1, Translated by K.A.K. Lott and E.L. Short. Chichester, West Sussex, UK: Ellis Horwood Limited, 1990.
- Stokesbury, James L. *A Short History of the Korean War*. New York: W. Morrow, 1988.
- Stoll, Clifford. *Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*. New York: Simon and Schuster, 2000.
- Stork, David G. (ed) and Arthur C. Clarke. *HAL's Legacy: 2001's Computer Dream and Reality*. Boston: MIT Press, 1998.
- Storz, Gisela, and Regine Hengge-Aronis. *Bacterial Stress Responses*. Washington: American Society for Microbiology Press, 2000.
- Strachan, T. and A. Read. *Human Molecular Genetics*. New York: Bios Scientific Publishers, 1998.
- Strong, Robert A. *Working in the World: Jimmy Carter and the Making of American Foreign Policy*. Baton Rouge: Louisiana State University Press, 2000.
- Stutman, Robert M., and Richard Esposito. *Dead on Delivery: Inside the Drug Wars, Straight from the Street*. New York: Warner Books, 1992.
- Survey of the Counterintelligence Needs of Private Industry*. Washington, D.C.: National Counterintelligence Center, 1995.
- Suvorov, Viktor. *Aquarium: The Career and Defection of a Soviet Spy*. London: Hamish Hamilton, 1985.
- Suvorov, Viktor. *Inside Soviet Military Intelligence*. New York: Macmillan, 1984.
- Syson, T. *Physics of Flying Things*. Philadelphia: Institute of Physics Publishing, 2003.
- Sze, S. *The Origins of the World Health Organization: A Personal Memoir*. Boca Raton: LISZ Publications, 1982.
- Szumski, Bonnie. *Latin America and U.S. Foreign Policy: Opposing Viewpoints*. St. Paul, MN: Greenhaven Press, 1988.
- Tarrant, V.E. *The Red Orchestra: The Soviet Spy Network Inside Nazi Europe*. New York: John Wiley and Sons, 1995.
- Taubman, Philip. *Secret Empire: Eisenhower, the CIA, and the Hidden Story of America's Space Espionage*. New York: Simon & Schuster, 2003.
- Taylor, A. W. B. *Superfluidity and Superconductivity*, 2nd ed. Bristol: Adam Hilger, 1986.
- Terrorism in the United States 1999*. Washington, D.C.: Federal Bureau of Investigation, 1999.
- Textbook of Medicine*. 19th ed. Philadelphia: W.B. Saunders, 1994.
- The EPCRA Compliance Manual: Interpreting and Implementing the Emergency Planning and Community Right-to-Know Act of 1986*. Chicago: American Bar Association Section of Environment, Energy, and Resources, 1997.
- Theoharis, Athan G. *A Culture of Secrecy: The Government Versus the People's Right to Know*. Lawrence: University of Kansas Press, 1998.
- Thief, Geoff. "Automatic CCTV Surveillance: Towards the VIRTUAL GUARD," in proceedings from the *International Carnahan Conference on Security Technology*, Larry D. Sanson, ed. 1999.
- Thomas, D. Brian. *Viruses and the Cellular Immune Response*. New York: Marcel Dekker, 1993.
- Thomas, Evan. *The Very Best Men—Four Who Dared: The Early Years of the CIA*. New York: Simon and Schuster, 1995.
- Thomas, Gordon. *Gideon's Spies: The Secret History of the Mossad*. New York: St. Martin's Press, 1999.
- Thompson, Kenneth W. *The President, the Bureaucracy, and World Regions in Arms Control*. Lanham, MD: University Press of America, 1998.
- Thompson, Kenneth W., ed. *The Reagan Presidency*. Lanham, MD: University Press of America, 1997.
- Thompson, Robert Smith. *The Missiles of October: The Declassified Story of John F. Kennedy and the Cuban Missile Crisis*. New York: Simon and Schuster, 1992.
- Thompson, Scott A. *Flight Check! The Story of FAA Flight Inspection*. Washington: DOT/FAA, Office of Aviation System Standards 1993.
- Thompson, Stephen P. *The War on Drugs: Opposing Viewpoints*. San Diego, CA: Greenhaven Press, 1998.
- Thomson, John F. *Biological Effects of Deuterium*. New York: Macmillan, 1963.
- Thornborough, Anthony M. *Sky Spies: Three Decades of Airborne Reconnaissance*. London: Arms and Armour Press, 1993.

- Todreas, Neil E., and Mujid S. Kazimi. *Nuclear Systems I: Thermal Hydraulic Fundamentals*. New York: Hemisphere Publishing Corporation, 1990.
- Toland, John. *In Mortal Combat, Korea, 1950–1953*. New York: Morrow, 1991.
- Tomedi, Rudy. *No Bugles, No Drums: An Oral History of the Korean War*. New York: Wiley, 1993.
- Tonry, Michael. *Malign Neglect: Race, Crime, and Punishment in America*. Oxford University Press, 1996.
- Tophoven, Rolf. *GSG 9, German Response to Terrorism*. Koblenz, Germany: Bernard & Graefe Verlag, 1984.
- Tourison, Sedgwick D. *Secret Army, Secret War: Washington's Tragic Spy Operation in North Vietnam*. Annapolis, MD: Naval Institute Press, 1995.
- Trask, Robert R., and Alfred Goldberg. *The Department of Defense, 1947–1997: Organization and Leaders*. Washington, D.C.: Office of the Secretary of Defense, 1997.
- Trask, Roger R. *Defender of the Public Interest: The General Accounting Office, 1921–1996*. Washington, D.C.: General Accounting Office, 1996.
- Trefil, James. *Encyclopedia of Science and Technology*. The Reference Works, Inc., 2001.
- Troy, Thomas F. *Donovan and the CIA: A History of the Establishment of the Central Intelligence Agency*. Frederick, MD: University Publications of America, 1981.
- Troy, Thomas F. *Wild Bill and Intrepid, Donovan, Stephenson, and the Origin of the CIA*. New Haven: Yale University Press, 1996.
- Tucker, J.B., (ed.). *Toxic Terror: Assessing the Terrorist Use of Chemical and Biological Weapons*. Cambridge: MIT Press, 2000.
- Tucker, Jonathan B. *The Once and Future Threat of Smallpox*. New York: Atlantic Monthly Press, 2001.
- Turner, Stansfield. *Secrecy and Democracy: The CIA in Transition*. Boston: Houghton Mifflin, 1985.
- Turvey, Brent E. *Criminal Profiling: An Introduction to Behavioral Evidence Analysis*. San Diego, CA: Academic Press, 1999.
- U.S. Central Intelligence Agency. Directorate of Intelligence. *The Russian Security Services: Sorting Out the Pieces*. Washington, D.C., 1992.
- U.S. Currency: Treasury's Plan to Study Genuine and Counterfeit U.S. Currency Abroad: Report to Congressional Requesters. Washington, D.C.: General Accounting Office, 1997.
- U.S. Department of State. *Foreign Relations of the United States: Department of State, 1945–1950*. Washington, D.C., 1996.
- U.S. Department of Transportation Research and Development Plan. Washington, D.C.: John A. Volpe National Transportation Systems Center, 1999.
- U.S. Government Printing Office. *Portals and Related Matters: Evidence Warranting Further Action by Federal Enforcement Authorities*. Washington, D.C.: U.S. Government Printing Office, 1999.
- Ullman, Harlan, James P. Wade, et al. *Shock and Awe: Achieving Rapid Dominance*. Washington, D.C.: Center for Advanced Concepts and Technology, 1996.
- Ullmann, John, and Steve Honeyman. *The Reporter's Handbook: An Investigator's Guide to Documents and Techniques*. New York: St. Martin's Press, 1983.
- Underwood, James R., Jr. and Peter L. Guth. *Military Geology in War and Peace*. Boulder, Colorado: Geological Society of America, 1998.
- United States Department of Justice and United States Department of the Treasury. *Interpol: The International Criminal Police Organization*. Washington, D.C.: Government Printing Office, 2002.
- United States Department of State, Bureau of Diplomatic Security. *Countering Terrorism: Security Suggestions for U.S. Business Representatives Abroad*. Washington, D.C.: Department of State, 1999.
- United States Department of State. *Foreign Relations of the United States*, Washington, D.C.: GPO, 1996.
- United States General Accounting Office National Security and International Affairs Division. *Ballistic Missile Defense: Evolution and Current Issues*. Washington, D.C.: United States General Accounting Office, 1993.
- United States General Accounting Office. *Chemical Safety Board: Improved Policies and Additional Oversight Are Needed*. Washington, D.C.: GPO, 2000.
- United States General Services Administration. Office of Federal Protective Service. *Careers in Security and Law Enforcement*. Washington, D.C.: Government Printing Office, 2002.
- United States General Services Administration. Public Buildings Service. Law Enforcement Division. *The Federal Protective Service*. Washington, D.C.: Government Printing Office, 1998.
- Venkus, Robert E. *Raid on Qaddafi: The Untold Story of History's Longest Fighter Mission by the Pilot Who Directed It*. New York: St. Martin's Press, 1992.
- Vinogradov, Ivan Matveevich. *Elements of Number Theory*. Dover Publications, 2003.
- Vise, David A. *The Bureau and the Mole: The Unmasking of Robert Philip Hanssen, the Most Dangerous Double Agent in FBI History*. New York: Atlantic Monthly Press, 2002.
- Vizzard, William J. *In the Cross Fire: A Political History of the Bureau of Alcohol, Tobacco, and Firearms*. Boulder, CO: Lynne Rienner, 1997.
- Volk, W., ed. *Basic Microbiology*, 7th ed. New York: Harper Collins, 1992.
- Volkman, Ernest. *Espionage: The Greatest Spy Operations of the Twentieth Century*. New York: John Wiley & Sons, 1996.
- Wagner, Günther, and Peter Van Den Haute. *Fission-Track Dating*. Boston: Kluwer Academic Publishers, 1992.
- Wagner, Henry N., and Linda E. Ketchum. *Living with Radiation: The Risk, the Promise*. Baltimore: The Johns Hopkins University Press, 1989.
- Wagnleitner, Reinhold. *Cocacolonization and the Cold War*. Chapel Hill, The University of North Carolina Press, 1997.
- Walker, J. Samuel, and George T. Mazuzan. *Containing the Atom: Nuclear Regulation in a Changing Environment, 1963–1971*. Berkeley: University of California Press, 1992.
- Walker, James W., and Steven Leroy De Vore. *Low Altitude Large-Scale Reconnaissance: A Method of Obtaining High Resolution Vertical Photographs for Small Areas*. Denver, CO: Interagency Archeological Services, National Park Service, 1995.
- Walker, William, and Frans Berkhout. *Fissile Material Stocks: Characteristics, Measures and Policy Options*. New York: United Nations, 1999.

- Wallace, John M. and Peter Hobbs. *Atmospheric Science: An Introductory Survey*. Orlando, Florida: Academic Press, Inc., 1977.
- Waller, John H. *The Unseen War in Europe: Espionage and Conspiracy in the Second World War*. New York: Random House, 1996.
- Walmer, Max. *An Illustrated Guide to Strategic Weapons*. New York: Prentice Hall Press, 1998.
- Walpole, Ronald, and Raymond Myers, et al. *Probability and Statistics for Engineers and Scientists*. Englewood Cliffs, NJ: Prentice Hall, 2002.
- Walston, Mark. *The Department of the Treasury*. New York: Chelsea House, 1989.
- Walters, Peter. "CCTV Operator Performance and System Design," in proceedings from the *International Carnahan Conference on Security Technology*, Larry D. Sanson, ed. 1993.
- Wang, Wallace. *Steal This Computer Book 3: What They Won't Tell You About the Internet*. San Francisco: No Starch Press, 2003.
- Warner, Michael. *The Office of Strategic Services: America's First Intelligence Agency*. Washington, D.C.: CIA History Staff, Center for the Study of Intelligence, 2000.
- Warner, Michael, ed. *The CIA Under Harry Truman*. Washington, D.C.: Center for the Study of Intelligence, 1994.
- Warner, Roger. *Backfire: The CIA's Secret War in Laos and Its Links to the Vietnam War*. New York: Simon & Schuster, 1995.
- Warren, Henry S., Jr. *Hacker's Delight*. Boston: Addison Wesley Professional, 2002.
- Waterson, A. and L. Wilkinson. *An Introduction of the History of Virology*. Cambridge: Cambridge University Press, 1978.
- Watson, Bruce W. *United States Intelligence: An Encyclopedia*. Washington, D.C.: CIA History Staff, Center for the Study of Intelligence, 2000.
- Watson, J.D., et al. *Molecular Biology of the Gene*, 4th ed. Menlo Park, CA: The Benjamin/Cummings Publishing Company, Inc., 1987.
- Weast, Robert C. *Handbook of Chemistry and Physics*. Cleveland, OH: CRC Press, 1975.
- Weber, Ralph E. ed. *Spymasters: Ten CIA Officers in Their Own Words*. Wilmington, Del: SR Books, 1999.
- Weber, Ralph E. ed. *Talking with Harry: Candid Conversations with President Harry S. Truman*. Wilmington, DE: SR Books, 2001.
- Webster, Daniel W. *Comprehensive Ballistic Fingerprinting of New Guns: A Tool for Solving and Preventing Violent Crime*. Baltimore, MD: Johns Hopkins Bloomberg School of Public Health, 2002.
- Weintraub, Stanley. *MacArthur's War: Korea and the Undoing of an American Hero*. New York: Free Press, 2000.
- Weitz, Margaret Collins. *Sisters in the Resistance: How Women Fought to Free France, 1940-1945*. New York: John Wiley & Sons., 1998.
- Wells, Tim. *Four Hundred and Forty-Four Days: The Hostages Remember*. Orlando, Florida: Harcourt Brace Jovanovich Publishers, 1985.
- Wentz, C. A. *Hazardous Waste Management*. New York: McGraw-Hill, 1989.
- Werrell, Kenneth P. *The Evolution of the Cruise Missile*. Maxwell Air Force Base, AL: Air University Press, 1985.
- Werrell, Kenneth P. *Hitting a Bullet with a Bullet: A History of Ballistic Missile Defense*. Maxwell AFB, AL: Air University Press, 2000.
- West, Nigel. *The Circus: MI5 Operations 1945-1972*. New York: Stein and Day, 1983.
- West, Nigel. *Molehunt: Searching for Soviet Spies in British Intelligence*. New York: Berkley, 1991.
- West, Nigel. *Molehunt: Searching for Soviet Spies in MI5*. New York: W. Morrow, 1989.
- West, Nigel. *The SIGINT Secrets: The Signals Intelligence War, 1900 to Today: Including the Persecution of Gordon Welchman*. New York: W. Morrow, 1988.
- West, Nigel and Oleg Tsarev. *The Crown Jewels*. London: Harper Collins Publishers, 1998.
- Westerby, Gerald. *In Hostile Territory: Business Secrets of a Mossad Combatant*. New York: HarperBusiness, 1998.
- Westerfield, H. Bradford, ed. *Inside the CIA's Private World: Declassified Articles from the Agency's Internal Journal*, New Haven, CT: Yale University Press, 1996.
- Westermeier, Reiner. *Electrophoresis in Practice*. Weinheim: Vch Verlagsgesellschaft, 2001.
- Whitcover, Jules. *Sabotage at Black Tom: Imperial Germany's Secret War in America, 1914-1917*; Chapel Hill, NC: Algonquin Books, 1989.
- White, Mark. *On the Control of Silencers, Interpol: The International Criminal Police Organization*. Washington, D.C.: Government Printing Office, 2002.
- White, Paul, ed. *Basic Microphones*. London: Sanctuary Press, 2000.
- White, William. *The Microdot: History and Application*. Williamstown: Phillips Publications, 1992.
- Whiting, Charles. *The Spymasters: The True Story of Anglo-American Intelligence Operations Within Nazi Germany, 1939-1945*. New York: Saturday Review Press, 1976.
- Whitnah, Donald Robert. *U.S. Department of Transportation: A Reference History*. Westport, CT: Greenwood Press, 1998.
- Whittaker, James A., and Herbert Thompson. *How to Break Software Security: Art and Science*. Boston: Addison Wesley Professional, 2002.
- Williams, John B. *Image Clarity: High-Resolution Photography*. Boston: Focal Press, 1990.
- Williams, Kieran, and Dennis Deletant. *Security Intelligence Services in New Democracies: The Czech Republic, Slovakia, and Romania*. New York: Palgrave, 2001.
- Willrich, Mason, ed. *International Safeguards and Nuclear Industry*. Baltimore, MD: Johns Hopkins Press, 1973.
- Wilson, E.J.N. *An Introduction to Particle Accelerators*. Oxford: Oxford University Press, 2001.
- Wilson, Jerry D. *Physics: Concepts and Applications*, 2nd edition. Lexington, MA: D. C. Heath and Company, 1981.

- Wilson, William. *Dictionary of the United States Intelligence Services: Over 1500 Terms, Programs, and Agencies*. Jefferson, NC: McFarland, 1996.
- Winks, Robin. *Cloak and Gown: Scholars in the Secret War*. New York: William Morrow and Company, Inc., 1987.
- Winter, Gordon. *Inside BOSS: South Africa's Secret Police*. London: Allen Lane, 1981.
- Winterbotham, F. W. *The Ultra Secret*. New York: Harper & Row, 1974.
- Winton, John. *Ultra in the Pacific: How Breaking Japanese Codes & Cyphers Affected Naval Operations against Japan: 1941–1945*. London: Leo Cooper, 1993.
- Wirtz, James J. *The Tet Offensive: Intelligence Failure in War*. Ithaca, NY: Cornell University Press, 1991.
- Wise, David. *Cassidy's Run: The Secret Spy War over Nerve Gas*. New York: Random House, Inc., 2000.
- Wise, David. *Spy: The Inside Story of How the FBI's Robert Hanssen Betrayed America*. New York: Random House, 2002.
- Witcover, Jules. *Sabotage at Black Tom: Imperial Germany's Secret War in America, 1914–1917*. Chapel Hill, NC: Algonquin Books, 1989.
- Witte, Robert S. *Statistics*. 3rd ed. New York: Holt, Rinehart and Winston, Inc., 1989.
- Wittkopf, Eugene R., and James M. McCormick. *The Domestic Sources of American Foreign Policy: Insights and Evidence*. Lanham, MD: Rowman and Littlefield Publishers, 1999.
- Wolf, Markus. *Man Without a Face: The Autobiography of Communism's Great Spymaster*. New York: Random House, 1997.
- Wolfson, Richard. *Nuclear Choices: A Citizen's Guide to Nuclear Technology*. Cambridge, Mass.: MIT Press, 1991.
- Woodward, Bob. *Maestro: Greenspan's Fed and the American Boom*. New York: Simon and Schuster, 2000.
- Wooldridge, E. T. *Carrier Warfare in the Pacific: An Oral History Collection*. Washington, D.C.: Smithsonian Institution Press, 1993.
- Woolfson, M.M. *An Introduction to X-Ray Crystallography*. Cambridge: Cambridge University Press, 1970.
- Wright, Peter. *Spycatcher: The Candid Autobiography of a Senior Intelligence Officer*. New York: Viking, 1987.
- Wright, Peter. *The Spycatcher's Encyclopedia of Espionage*. Richmond and Victoria: William Heinemann Australia, 1991.
- Wright, Robert K. *Military Police*. Washington, D.C.: Center of Military History, 1992.
- Wyngaarden, J.B., L.H. Smith, Jr., and J.C. Bennett. *Cecil Textbook of Medicine*, 19th ed. Philadelphia: W.B. Saunders, 1992.
- Wynne, Greville. *The Man from Moscow: The Story of Wynne and Penkovsky*. London: Hutchinson, 1967.
- Yardley, Herbert O., *The American Black Chamber*. Indianapolis: Bobbs-Merrill, 1931.
- Yinon, Jehuda. *Forensic and Environmental Detection of Explosives*. New York: John Wiley & Sons, 1999.
- Yoder, Andrew R., and Hank Bennett. *The Complete Shortwave Listener's Handbook*. New York: McGraw-Hill, 1997.
- Young, Gray. *The Internet*. New York: H. W. Wilson, 1998.
- Zacharias, Ellis M. *Secret Missions: The Story of an Intelligence Officer*. New York: G. P. Putnam's Sons, 1946.
- Zegart, Amy B. *Flawed by Design: The Evolution of the CIA, JCS, and NSC*. Stanford, CA: Stanford University Press, 1999.
- Zen, E-An and A. S. Walker. *Rocks and War: Geology and the Civil War Campaign of Second Manassas*. Shippensburg, Pennsylvania: White Mane Publishing, 2000.
- Zim, Herbert Spencer. *Codes and Secret Writing*. New York: W. Morrow, 1948.
- Zimmerman, Phillip. *The Official PGP User's Guide*. Cambridge, MA: MIT Press, 1995.
- Zukin, Sharon. *Landscapes of Power: From Detroit to Disney World*. Berkeley: University of California Press, 1991.

## Periodicals

- Adams, Shawn. "A Beginner's Guide to Learning Emergency Management." *Risk Management* 49, no. 5 (May 2002): 24–28.
- Advisory Committee on Immunization Practices. "Recommendations of the Advisory Committee on Immunization Practices: Use of Anthrax Vaccine in the United States." *Morbidity and Mortality Weekly Report* no. 49 (2000): 1–20.
- "Agency Says Engineers Likely Broke Rules." *Washington Post*. (February 29, 2000): A4.
- Ahrens, Frank. "Submarines, Examined at Depth: The Smithsonian's New Nautical Exhibit Settles in for a Three-Year Tour." *Washington Post*. (May 8, 2000): C1.
- Alden, Edward, and James Harding. "CIA Wins Battle to Defend U.S. Against Terror." *Financial Times*. (February 15, 2003): 1.
- Alden, Edward, and Mark Turner. "Sudan's Surprise Deal with Rebels Catches Washington Off-Guard." *Financial Times*. (July 23, 2002): 10.
- Alexander, Leo. "Medical Science Under Dictatorship." *New England Journal of Medicine* 241, no. 2 (1949): 39–47.
- Allen, Deane J. "Reviewing the Literature: Intelligence Is Organization." *Defense Intelligence Journal* no. 1 (Spring 1992): 113–120.
- Allen, Gary W., and Anthony J. Ramienski. "A Survey of Intelligence Literature." *Military Intelligence* 12, no. 2 (1986): 54–56.
- Alouf, J.E. "From Diphtheritic Poison to Molecular Toxinology." *American Society for Microbiology News*, vol. 53, no. 10 (1987): 547–551.
- Alper, Joseph. "Navigating Chernobyl's Deadly Maze." *Science* 5365 (May 8, 1998): 826–827.
- Altmann, Jürgen. "Acoustic Weapons—A Prospective Assessment." *Science and Global Security* no. 9 (2001): 165–244.
- Amar, A.R. "A Search For Justice In Our Genes." *New York Times*. 7 May 2002: A31.
- Amon, Michael. "Agencies Working to Boost Security." *Washington Post*. (February 23, 2003): T1.
- Anderson, Robert. "The Former Soviet Republics Are Accused of Supplying Weapons to Rogue States in Defiance of United Nation or U.S. Embargoes." *Financial Times*. (October 21, 2002): 27.
- Arkin, William M. "Sci-Fi" Weapons Going to War." *Los Angeles Times*. (December 8, 2002): M1.



- Arlt, R., et al. "Use of CdZnTe Detectors in Hand-Held and Portable Isotope Identifiers to Detect Illicit Trafficking of Nuclear Material and Radioactive Sources." *Nuclear Science Symposium Conference Record*, vol. 1, IEEE, 2001: 4-18-4-23.
- Arney, Kevin. "Midshipman Cruises Aboard Fast Attack Submarine." *The Officer* 73, no. 11 (November 1997): 57.
- Astakhova, L.N., L.R. Anspaugh, G.W. Beebe, et al. "Chernobyl-Related Thyroid Cancer in Children in Belarus." *Radiation Research* no. 150 (1998): 349-356.
- Atlas, R.N. "National Security and the Biological Research Community." *Science* no. 298 (2002): 753-754.
- Auer, Catherine. "EU Knocks Echelon, Wants Own Super Spy." *Bulletin of the Atomic Scientists* 57, no. 5 (September/October 2001): 11.
- Auerbach, Stuart. "Party Nominees to Get Trade Briefing." *Washington Post*. (June 25, 1988): D12.
- Aveni, Madonna. "Software Analyzes Potential Threats to Buildings." *Civil Engineering* 71, no. 10 (October 2001): 36.
- Babbin, Jed. "Some Things Can't Wait: Speedy Approval of New Military Technologies Will Save Lives." *Washington Times*. (June 27, 2002): A23.
- Bakalar, James B. "The War on Drugs: A Peace Proposal." *The New England Journal of Medicine* (Feb 3 1994): 357-61.
- Baker, Stewart A. "Don't Worry, Be Happy: Why Clipper Is Good for You." *Wired*. June 1994.
- Baldauf, Scott. "Where to Find the Perfect Gift for Your 007 Wannabe." *Christian Science Monitor*. (December 7, 1999): 2.
- Balding, D.J. "The DNA Database Search Controversy." *Biometrics* 58(1): 241-4 (March 2002).
- Ballard, Tanya N. "Horror, then a Helping Hand." *Government Executive* 33, no. 13 (October 2001): 12-14.
- Banerjee, Neela. "U.S. and Europe in Fuel Cell Pact." *New York Times*. March 7, 2003.
- Barinaga, Marcia, "Asilomar Revisted: Lessons for Today?" *Science* 287 (2000).
- Barnes, Scottie. "State Department Hosts Forum on Geographic Information." *Geospatial Solutions* 12, no. 9 (September 2002): 18.
- Barr, Stephen. "Defense Department Agrees to Have OPM Take over Background Checks." *Washington Post*. (February 5, 2003): B2.
- Barr, Stephen. "Probe's Findings Support INS Whistleblower." *Washington Post*. (December 16, 1998): A29.
- Barth, Steve. "Spy vs. Spy." *World Trade* 11, no. 8 (August 1998): 34-37.
- Baus, Theresa. "Dual Use Technology." *Naval Forces* 20, no. 3 (1999): S54-S55.
- Baxevanis, A.D. "The Molecular Biology Database Collection: An Updated Compilation of Biological Database Resources." *Nucleic Acids Research* 29 (January 2001): 1-10.
- Begley, S. "The End of Antibiotics." *Newsweek*. (28 March 1994): 47-51.
- Behnisch P.A. "Biodetectors in Environmental Chemistry: Are We at a Turning Point?" *Environ Int.* 27(2001):441-2.
- Belgrader, P., W. Bennet, D. Hadley, et al. "PCR Detection of Bacteria in Seven Minutes." *Science*. no. 5413: 449-450
- Bennett, Charles H., and David P. DiVincenzo. "Quantum Information and Computation." *Nature* 404 (March 16, 2000): 247-255.
- Bennett, Charles H., and Peter W. Shor. "Privacy in a Quantum World." *Science* no. 5415 (1999): 747-748.
- Bennewitz, R., et al. "Atomic scale memory at a silicon surface." *Nanotechnology* 13 (2000): 499-502.
- Berg, P., et al. "Asilomar Conference on Recombinant DNA Molecules." *Science* no. 188 (6 June 1975): 991-994.
- Bethe, Hans A., et al. "Space-Based Ballistic-Missile Defense." *Scientific American*. (October, 1984).
- Betsch, D.F. "DNA Fingerprinting in Agricultural Genetics Programs." *Biotechnology Information Series (Bio-7)*, North Central Regional Extension Publication. Iowa State University 1994.
- Betts, K.S. "DNA Chip Technology Could Revolutionize Water Testing." *Environmental Science and Technology* no. 33 (1999): 300A-301A.
- "Black September 11." *Air Force Magazine* 95, no. 9 (September 2002): 46-53.
- Black, Chris. "Mitchell Urges New Classified Data Law." *Boston Globe*. (December 5, 1989): 3.
- Blair, Jayson. "C.I.A. Chief Slips in to Study Police Department Program." *New York Times*. (November 6, 1999): section B, p. 2.
- Bland, Timothy S. "Background Checks: Making a Federal Case." *Journal of Property Management* 64, no. 5 (September/October 2000): 26-31.
- Bleek, Philipp C. "New DOE Nuclear Security Organization Begins Work." *Arms Control Today* 30, no. 3 (April 2000): 29-30.
- Blumenstein, Rebecca, and Matthew Rose. "Name That Op: How U.S. Coins Phrases of War." *Wall Street Journal*. (March 24, 2003): B1.
- Bodrain, Rosemarie R. "Analysis of Exempt Paint Solvents by Gas Chromatography Using Solid-Phase Microextraction." *JCT, Journal of Coatings Technology* 72, no. 900 (January 2000): 69-74.
- Boguski, M.S. "The Turning Point in Genome Research." *Trends in Biochemical Sciences* 20 (August 1995): 295-296.
- Bone, Margaret. "Marines Provide Safety Net to Terrorist Threat." *Leatherneck* 82, no. 2 (February 1999): 50-53.
- Bonner, Raymond, et al. "Questioning Terror Suspects in a Dark and Surreal World." *New York Times*. (March 9, 2003): 1.
- Bowman, M. E. "Intelligence and International Law." *International Journal of Intelligence and Counterintelligence* 8, no. 3 (fall 1995): 321-335.
- Boylan, M. "Genetic Testing." *Camb Q Healthc Ethics* Summer 2002;11(3): 246-56.
- Boyle, Matthew. "The Prying Game." *Fortune*. 144, no. 5 (September 17, 2001): 235.
- Boyne, Sean. "Assad Purges Security Chiefs to Smooth the Way for Succession." *Jane's Intelligence Review* 11, no. 6 (June 1, 1999): 1.
- Bradley, K.A., J. Mogridge, M. Mourey, et al. "Identification of the Cellular Receptor for Anthrax Toxin." *Nature* no. 414 (2001): 225-229.

- Braga, Newton C. "Experimenting with Small FM Transmitters." *Poptronics* 2, no. 9 (September 2001): 41–46.
- Brainard, Jeffrey. "Profiles in Pork: Wheeling Jesuit University: National Technology Transfer Center." *The Chronicle of Higher Education* 49, no. 5 (September 27, 2002): A23.
- Brand, Lois. "Helping Coast Guard Enhance Port Security." *National Defense* 87, no. 590 (January 2003): 45.
- Brinkley, Joel. "Coast Guard Encounters Big Hurdles in New Effort to Screen Arriving Ships." *New York Times*. (March 16, 2002): A9.
- Brouwer, Greg. "Oklahoma City Complex Will Usher in New Design Criteria." *Civil Engineering* 72, no. 3 (March 2002): 16.
- Brugioni, Dino A. "Satellite Images on TV: The Camera Can Lie." *Washington Post*. December 14, 1986.
- Brunet, D., and D.A. Yuen. "Mantle Plumes Pinched in the Transition Zone." *Earth and Planetary Science Letters*, vol. 178 (2000): 13–27.
- Bruning, Horst, and Stephen Wolff. "Automated Explosive Detection Systems Based Upon CT Technology." *Security Technology, 1998. Proceedings., 32nd Annual 1998 International Carnahan Conference*. Oct. 12–14, 1998: 55–58.
- Buck, S. "Searching for Graves Using Geophysical Technology: Field Tests with Ground Penetrating Radar, Magnetometry, and Electrical Resistivity." *Journal of Forensic Sciences*, vol. 48, no. 1 (2003): 5–11.
- Bumiller, Elisabeth. "Government to Cover Most Costs of Insurance Losses in Terrorism." *New York Times*. (November 27, 2002): A1.
- Burke, Jim. "Kids, Drugs, and Bureaucrats." *Washington Post*. (May 21, 2002): A17.
- Burns, Jimmy. "Assessing Terror Threat Raises Whitehall Tension." *Financial Times*. (December 14, 2002): 5.
- Burrows, W.D., and S.E. Renner. "Biological Warfare agents as Threats to Potable Water." *Environmental Health Perspectives* no. 107 (1999): 975–984.
- Bush, George W. "Remarks on Signing the Terrorism Risk Insurance Act of 2002." *Weekly Compilation of Presidential Documents* 38, no. 48 (December 2, 2002): 2096–2097.
- Bush, George W. "Statement on Signing the Intelligence Authorization Act for Fiscal Year 2002." *Weekly Compilation of Presidential Documents* 37, no. 52 (December 31, 2001): 1834.
- Byrne, M.P., and L.A. Smith. "Development of Vaccines for Prevention of Botulism." *Biochimie* no. 82 (2000): 955–966.
- Cabellon, Paul C. "CBIRF Takes the (Capitol) Hill." *Leatherneck* 85, no. 2 (February 2002): 19.
- Caipo, M.L., S. Duffy, L. Zhao, et al. "Bacillus megaterium Spore Germination is Influenced by Inoculum Size." *Journal of Applied Microbiology* no. 92 (2002): 879–884.
- Campbell, Duncan. "U.S. Buys Up All Satellite War Images." *The Guardian (London)*. October 17, 2001.
- Campbell, Kurt M. "Edging Taiwan in from the Cold." *Washington Post*. (April 25, 2001): A31.
- Cannon, Carl M. "Central Intelligence Agency." *National Journal* 33, no. 25 (June 23, 2001): 1903–1904.
- Cao, Y.W.C., R. Jin, and C.A. Mirkin. "Nanoparticles with Raman Spectroscopic Fingerprints for DNA and RNA Detection." *Science* no. 5586 (2002): 1536–1540.
- Carlson, Caron. "No Threat from GSM Hackers." *Wireless Week* 5, no. 50 (December 13, 1999): 3.
- Carr, Chris, Jerry Furniss, and Jack Morton. "Complying with the Economic Espionage Act." *Risk Management* 47, no. 3 (March 2000): 21–24.
- Carr, Rebecca. "Security at Nuke Labs Lax—DOE 'Indifferent' Despite Sept. 11." *Atlanta Journal-Constitution*. (August 20, 2002): A11.
- Casagrande, R. "Technology Against Terror." *Scientific American*. 287 (2002):59–65
- Caterinicchia, Dan. "When Duty Calls." *Federal Computer Week* 16, no. 36 (October 7, 2002): 25–26.
- Chalmers, Bruce. "The Photovoltaic Generation of Electricity." *Scientific American*. 235, no.4 (October 1976): 34–43.
- Champion, Marc. "How Do Other Countries Coordinate Security?" *Wall Street Journal*. (June 12, 2002): A14.
- Chapman, Gary. "U.S.-British Cyber-Spy System Puts European Countries on Edge." *Los Angeles Times*. (August 16, 1999): 3.
- Charles, Douglas M. "American, British and Canadian Intelligence Links: A Critical Annotated Bibliography." *Intelligence and National Security* 15, no. 2 (Summer 2000): 259–269.
- Cho, A. "Forensic Science. Judge Reverses Decision On Fingerprint Evidence." *Science* March 2002;295(5563):2195–7.
- Choffnes, E. "Germs on the Loose." *Bulletin of the Atomic Scientists* no. 57 (2001): 57–61.
- Cholewka, Kathleen. "Address Management Made Easier?" *Telephony* 234, no. 1 (January 5, 1998): 39.
- "Circuit Transfers Four Times More Power Out of Vibration." *Resource* 9, no. 11 (November 2002): 6.
- Clellenad, C.T., V. Risca, and C. Bancroft. "Hiding Messages in DNA Microdots." *Nature* no. 399 (1999): 533–534.
- Cloud, David S. and David Rogers. "Telecom Firms Lobby for Funding of Upgrades to Ease Surveillance." *Wall Street Journal*. (April 5, 2000): A4.
- Cochran, William W. "Direction Finding at Ultra High Frequency (UHF): Improved Accuracy." *Wildlife Society Bulletin* 29, no. 2 (Summer 2001): 594.
- Collins F.S., and V.A. McKusick. "Implications of the Human Genome Project for Medical Science." *JAMA* 285 (7 February 2001): 540–544.
- Comello, Vic. "Researchers Are Giving SPME a Second Look." *Research & Development* 41, no. 2 (February 1999): 44–45.
- Connolly, P. J. "Fight DDoS Attacks with Intelligence." *InfoWorld* 23, no. 39 (September 24, 2001): 58.
- Costigliola, Frank. "Unceasing Penetration": Gender, Pathology, and Emotion in George Kennan's Formation of the Cold War." *Journal of American History* 83 (March, 1997): 1309–1939.
- Crabb, C. "Biosensors Enliven the Science of Detection." *Chemical Engineering* August (1998): 35–39.
- Crabb, Peter B. "The Use of Answering Machines and Caller ID to Regulate Home Privacy." *Environment and Behavior* 31, no. 5 (September 1999): 657–670.
- Crawford, David. "Europe Eases Limits on Police, Intelligence Services—Fear of Islamist Terrorism Erodes Traditional Divide Between the Two Branches." *Wall Street Journal*. (December 17, 2002): A15.

- Crawley, James W. "Details of Port Security Are Off-Limits." *San Diego Union-Tribune*. (August 23, 2002): B1.
- "Crime Year in Review." *Crime Control Digest* 36, no. 35 (August 30, 2002): 1.
- Croft, John. "Air Security Bill Clears Lawmakers' Logjam." *Aviation Week & Space Technology* 155, no. 21 (November 19, 2001): 46.
- Csonka, E, et al. "Novel Generation of Human Satellite DNA-based Artificial Chromosomes in Mammalian Cells." *Journal of Cell Science* 113 (2000): 3207–3216.
- Cummings, Jeanne, and Gary Fields. "Calculating Risks: For Two Tense Days, Bush Team Wrestled with Vague Threat." *Wall Street Journal*. (May 17, 2002): A1.
- Dao, James. "Nuclear Study Raises Fears About Weapon." *New York Times*. (November 17, 2002): section 1, p. 22.
- Darce, Keith. "Port Still Vulnerable, Its Chief Says." *Times-Picayune (New Orleans, LA)*. (November 20, 2002): 1.
- Darlington, C. D., and T.D. Lysenko (Obituary). *Nature* 266 (1977): 287–288.
- DaSilva, E. "Biological Warfare, Terrorism, and the Biological Toxin Weapons Convention." *Electronic Journal of Biotechnology* 3(1999): 1–17.
- Daughtry, Emily Ewell, and Fred L. Wehling. "Cooperative Efforts to Secure Fissile Material in the NIS." *Nonproliferation Review* 7, Spring 2000.
- "Deadline Met for Airport Security Screeners." *San Diego Union-Tribune*. (November 17, 2002): A2.
- Dean, Jason. "Taipei's Turmoil Hinders Action on Key Issues." *Wall Street Journal*. (March 21, 2002): A18.
- Demmig-Adams, B., and W.W. Adams III. "Photosynthesis: Harvesting Sunlight Safely." *Nature* 403; (January 2000): 371–374.
- Dempsey, D.A., H. Silva, and D.F. Klessig. "Engineering Disease and Pest Resistance in Plants." *Trends in Microbiology* no. 6 (June 1998): 54–61.
- Dempsey, Judy. "EU Military Mission at Risk from Turkish Rift." *Financial Times*. (September 19, 2002): 12.
- Dennis, D.T. "Tularemia." *Maxcy-Rosenau-Last Public Health and Preventive Medicine*, 14th edition. Edited by R.B. Wallace. Stamford: Appleton & Lange, 1998.
- Dennis, D.T., et al. "Tularemia as a Biological Weapon." *Journal of the American Medical Association* no. 285 (June 2001): 2763–2773.
- Dennis, D.T., N. Gratz, J.D. Poland, and E. Tikhomirov. *Plague Manual: Epidemiology, Distribution, Surveillance and Control*. Geneva: World Health Organization, 1999.
- Denton M.D., T. Yoshida, L.L. Hsiao, R.V. Jenson, and S.R. Gullans. "DNA Microarrays: Applicability To Renal Physiology And Disease." *J. Nephrol* 2002 Mar-Apr;15 Suppl 5:S184–91.
- "Designed for Danger." *Design News* 55, no. 2 (January 17, 2000): 28.
- Deutch, John. "Smarter Intelligence." *Foreign Policy* no. 128 (January/February 2002): 64–69.
- DeYoung, K., and Colum Lynch. "Britain Races To Rework Resolution: U.S. Insists on Limiting Concessions for Iraq." *Washington Post*. March 11, 2003.
- Dezelan, Louis A. "Preparing for Terrorism." *Law & Order* 46, no. 10 (October 1998): 107–110.
- Diaz-Mitoma, F., S. Paton, and A. Giulivi. "Hospital Infection Control and Bloodborne Infective Agents." *Canada Communicable Disease Report* no. 27S3 (September 2001): 40–45.
- Dietrich, Bill. "Engineering—Here's What You Can Expect Next Century." *Seattle Times*. (December 15, 1992): D1.
- Dire, D.J., and T.W. McGovern. "CBRNE—Biological Warfare Agents." *eMedicine Journal* 4(2002):1–39.
- Dominique, Dean J. "Convoy Rat Patrol." *Army Logistician* 34, no. 3 (May/June 2002): 36–37.
- Donnelly, John. "N. Korean Missile Has U.S. Range." *Boston Globe*. (February 13, 2003): A1.
- Donnelly, Sally B. "Grounding the Air Marshals." *Time*. 161, no. 4 (January 27, 2003): 17.
- Doolling, Dave. "Space Sentries." *IEEE Spectrum* (September, 1997): 50–59.
- Duchak, G. D. "Discoverer II: A Space Architecture for Information Dominance." *Aerospace Conference Proceedings* (Vol. 7), IEEE, 1998: 9–17.
- Duffy, Brian. "Terror in the Gulf: Bombs in the Desert" *U.S. News & World Report*. July 8, 1996: 28–32.
- Dunlap, David W. "Architects Put on the Alert over Requests That Are Rare." *New York Times*. (October 4, 2001): B8.
- Dutton, Gail. "Biotechnology Counters Bioterrorism." *Genetic Engineering News* no. 21 (December 2000): 1–22ff.
- Eaglesham, Jean. "Bad Smells" Could Be Used to Disperse Crowds." *Financial Times*. (October 31, 2002): 3.
- "Early Warning Technology." *Med Device Technol* 13 (2002): 70–2.
- "EDM on Mission to Mars." *Manufacturing Engineering* 119, no. 4 (October 1997): 116.
- Eggen, Dan, and Jim McGee. "FBI Rushes to Remake Its Mission: Counterterrorism Focus Replaces Crime Solving." *Washington Post*. (November 12, 2001): A1.
- Eggen, Dan. "Bush Aims to Blend Counterterrorism Efforts." *Washington Post*. (February 15, 2003): A16.
- Eggen, Dan. "FBI Seeks Data on Foreign Students; College Calls Request Illegal." *Washington Post*. (December 25, 2002): A1.
- Eggen, Dan. "Hijackers Got Visas with Little Scrutiny, GAO Reports." *Washington Post*. (October 22, 2002): A7.
- Elvin, John. "We've Waited Long Enough." *Washington Times*. (December 27, 1999): 26.
- "E-mail and Patching Hints from NIST." *Security Management* 46, no. 7 (July 2002): 44.
- Engelhard, Victor H. "How Cells Process Antigens." *Scientific American*. 271 (August 1994): 54.
- Enserink, M. "Anthrax Sequence. Useful Data But No Smoking Gun." *Science* 296(5570), (May 2002): 1002–3.
- "EPA Security Plan for Refining, Chemical Plants Blasted." *Oil & Gas Journal* 100, no. 39 (September 23, 2002): 22–24.
- Epidemiology Program Office, CDC. "CDC's 50th Anniversary: History of CDC." *Morbidity and Mortality Weekly Report* no. 45 (1996): 525–30.

- Epstein, Edward. "U.S. Has New Weapon Ready." *San Francisco Chronicle* (February 14, 2003): A1.
- Ernst, Maurice. "Economic Intelligence in CIA," *Studies in Intelligence* 28, no. 4 (Winter 1984): 1–16.
- Evans, D., and D. Charter. "Iraq Strikes Back with Suspected Banned Missiles." *The Times*. March 21, 2003.
- Evans, J.P.O., M. Robinson, and S.X. Godber. "Pseudo-Tomographic X-Ray Imaging for Use in Aviation Security." *IEEE AES Systems Magazine*, July 1998.
- Evers, Joris. "U.S. Spy Technology Failed to Signal Attack Planning." *InfoWorld* 23, no. 38 (September 17, 2001): 28.
- Evers, Stacey. "DARPA to Reap Benefits of 'Energy Harvesting'." *Jane's Defence Weekly* (November 26, 1997): 8.
- Fanton, Ben. "View from Above the Battlefield." *America's Civil War* 14, no. 4 (September 2001): 22–28.
- Farson, S.A. "Is Canadian Intelligence Being Re-Invented?" *Canadian Foreign Policy* no. 6 (1999): 49–83.
- Feder, Barnaby J. "Truth and Justice, By the Blip of a Brainwave." *New York Times*. (October 9, 2001): F3.
- "FERC Streamlining to Reflect Industry." *Oil & Gas Journal* 96, no. 26 (June 29, 1998): 33.
- Ferdinand, P. "Would-Be Shoe Bomber Gets Life Term." *Washington Post*. January 31, 2003; Page A1.
- Ferris, John. "Coming In from the Cold War: The Historiography of American Intelligence, 1945–1990." *Diplomatic History* 19, no. 1 (Winter 1995): 87–115.
- Fialka, John J. "Aftermath of Terror: Rules for Hiring Agents Are Criticized as Hampering Spy Agencies' Recruiting." *Wall Street Journal*. (September 13, 2001): A13.
- "Firms Are Lining up to See." *Electronic Times* (October 16, 2000): 40.
- Fisher, I. "Chief Weapons Inspectors See No Big Breakthrough After Talks in Baghdad." *New York Times*. February 10, 2003.
- Flatter, J. R. "Military Police: A Force of Choice for the 21st Century MEU (SOC)." *Marine Corps Gazette* 81, no. 7 (July 1997): 36.
- Foran, J.A., and T.M. Brosnan. "Early Warning Systems for Hazardous Biological Agents in Potable Water." *Environmental Health Perspectives* no. 108 (2000): 993–996.
- Forde, Geoffrey, Pavel Podvig, and Theodore A. Postol. "False Alarm, Nuclear Danger." *IEEE Spectrum* (March, 2000): 31–39.
- Fowler, Charles. "National Missile Defense (NMD)." *IEEE Aerospace and Electronic Systems Society (AESS) Systems Magazine* (January, 2002): 4–12.
- Frank, Diane. "Cybersecurity Center Takes Shape." *Federal Computer Week* 16, no. 4 (February 18, 2002): 10.
- Frank, Diane. "GSA Preps Security Pacts." *Federal Computer Week* 13, no. 6 (March 15, 1999): 1.
- Frank, Diane. "NIST Aims Grants at Systems Security." *Federal Computer Week* 15, no. 11 (April 23, 2001): 12.
- Frankel, Max. "Learning From the Missile Crisis." *Smithsonian* October, 2002: 53–64.
- French, M. "Retinal Eyes Biometric Security. Company Reveals its Scanning Technology." *Mass High Tech. The Journal of New England Technology* 32 (2001).
- Friedlander, A.M. "Tackling Anthrax." *Nature* no. 414 (2001): 160–161.
- Fulghum, David A. "Microwave Weapons May Be Ready for Iraq." *Aviation Week & Space Technology* 157, no. 6 (August 5, 2002): 24.
- Fund, John. "In the Fray: People Spotters—European Gizmo Tells Who's Who." *Wall Street Journal*. (January 23, 2003): D8.
- Gaddis, John Lewis. "A Grand Strategy for Transformation." *Foreign Policy* no. 133 (November/December 2002): 50–57.
- Garamone, Jim. "Marines to Stand up Anti-Terror Brigade." *Pentagon Brief* (October 2001): 5.
- Garritsen De Vries, Margaret. "The IMF Fifty Years Later." *Finance & Development* June 1995: 43–47.
- Garth, Jeff. "Retired General to Oversee Nuclear Weapons Labs." *New York Times*. (June 17, 1999): A15.
- Garvey, William. "Rebirth of the Blimp." *Popular Mechanics*. 168 (1991): 30–33.
- Gellman, Barton. "Cyber-Attacks by Al Qaeda Feared." *Washington Post*. (June 27, 2002): A1.
- Gerard, S., M. Hayes, and M. A. Rothstein. "On the Edge of Tomorrow: Fitting Genomics Into Public Health Policy." *Journal of Law, Medicine and Ethics* no. 30(3 Suppl) (2002): 173–176.
- Gill, Peter. Review of *Security Intelligence Services in New Democracies: The Czech Republic, Slovakia, and Romania*. *Slavic Review* 61, no. 2 (2002): 375–376.
- Giodano, Vincent. "Is It Right for Your Company?" *Communications News* 37, no. 9 (September 2000): 66–68.
- Gips, Michael A. "Options Reviewed for Federal Building Security." *Security Management* 46, no. 7 (July 2002): 14.
- Gips, Michael A. "They Secure the Body Electric." *Security Management* 46, no. 11 (November 2002): 77–81.
- Girardeau, John H. "Doctrine Corner: INSCOM Intelligence Support to the Tactical Commander." *Military Intelligence Professional Bulletin* 28, no. 2 (April-June 2002): 56–57.
- Gladwell, Martin. "Safety in the Skies." *New Yorker*. October 1, 2002.
- Golden, Tim. "White House Wary of Cuba's Little Spy Engine That Could." *New York Times*. (January 5, 2003): p. 1, 3.
- Goo, Sara Kehaulani. "Security Law Called Unconstitutional." *Washington Post*. (November 16, 2002): A12.
- Goodman, Melvin A. "Science at the CIA." *Issues in Science and Technology* 18, no. 3 (Spring 2002): 90–93.
- Gordievsky, Oleg. "The KGB Archives." *Intelligence and National Security* 6, no. 1 (Jan. 1991): 7–14.
- Gordon, Michael R. "Radio Transmitter to Oppose Hussein Wins U.S. Support." *New York Times*. (February 28, 2002): A1.
- Gordon, Michael R. "U.S. Arsenal: Treaties vs. Nontreaties." *New York Times*. (November 14, 2001): A12.
- Gorman, Tom. "Rescue Worker Boot Camp." *Los Angeles Times*. (October 11, 2001): A6.
- Gottlieb, Daniel W. "Keeping Trade Secrets Secret: Counterspies, Codes Courts." *Purchasing* 126 no. 7 (May 6, 1999): 24–25.
- Grant, Peter. "Plots and Ploys." *Wall Street Journal*. (December 26, 2001): B4.

- Greenberger, Robert S. "Dictating Terms: Sept. 11 Aids Gadhafi in Effort to Get Libya off U.S. Terrorist List." *Wall Street Journal*. (January 14, 2002): A1.
- Greenfield, Ronald A. "Microbiological, Biological, and Chemical Weapons of Warfare And Terrorism." *American Journal of The Medical Sciences* 323, no. 6 (2002): 326–340.
- Grier, Peter. "Hypersonic Aircraft Test Fails." *Air Force Magazine* 84, no. 8 (August 2001): 17.
- Griffiths, A., et al. *Introduction to Genetic Analysis*, 7th ed. New York: W.H. Freeman and Co., 2000.
- Grimm, Matthew. "A Dubious Pitch." *American Demographics* 24, no. 5 (May 2002): 44–46.
- Grimsted, Patricia Kennedy. "Archives of Russia Seven Years After: 'Purveyors of Sensation or Shadows of the Past?'" *Cold War International History Project Working Paper*, no. 20, Part I. Washington, DC: CWIHP (1998).
- Grimsted, Patricia Kennedy. "Russian Archives in Transition: Caught Between Political Crossfire and Economic Crisis." *The American Archivist* 56, no. 4 (Fall 1993): 618–619.
- Grunwald, Michael. "Former FBI Workers File Whistleblower Suit." *Washington Post*. (October 20, 1998): A17.
- Hafele, Wolf. "Energy from Nuclear Power," *Scientific American*. 263: 136–144, September, 1990.
- "Hainan Incident Increases Pressure in Sino-U.S. Relations." *Defense Daily International* 1, no. 2 (April 6, 2001): 14.
- Hall, Mimi. "Preparations Underway for Radiation Attack." *USA Today*. (July 8, 2002): A2.
- Hamer, Mick. "Airships Face a Military Future." *New Scientist* 115 (1987): 38–40.
- Haque, M. Shamsul. "Government Responses to Terrorism: Critical Views of Their Impacts on People and Public Administration." *Public Administration Review* 62 (September 2002): 170–180.
- Harney, R.C. "Physics and Technology of Coherent Infrared Radar." *Proceedings of the SPIE*, vol. 300 (1981).
- Harris, J. "Ethical Issues in Genetic Testing for Insurance." *Law Hum Genome Rev.* 2001 Jul-Dec;(15):25–31.
- Harvey, Bernard G. "Criteria for the Discovery of Chemical Elements." *Science* 193 (1976): 1271–2.
- Haskell, Bob. "A Plan Well-Executed." *Soldiers* 53, no. 5 (May 1998): 38.
- Haynes, V. Dion. "U.S. Works to Shore up Port Security; War Game Underscores Acute Risk." *Chicago Tribune*. (March 10, 2003): 8.
- Hays, Daniel. "One-Size-Fits-All Doesn't Fit: Study." *National Underwriter* 107, no. 9 (March 3, 2003): 26.
- Healy, Melissa. "Doomsday Plane's Round-the-Clock Flights Called Off." *Los Angeles Times*. (July 28, 1990): 2.
- Henderson J.P. "The Use Of DNA Statistics In Criminal Trials." *Forensic Sci Int.* 2002 Aug 28;128(3):183–6.
- Henderson, D.A. "Smallpox: Clinical and Epidemiologic Features." *Emerging Infectious Diseases* no. 5 (1999): 537–539.
- Henderson, D.A., "The Looming Threat of Bioterrorism." *Science* no. 283 (1999): 1279–1282.
- Henderson, D.A., T.V. Inglesby, J.G. Bartlett, et al. "Smallpox as a Biological Weapon: Medical and Public Health Management." *Journal of the American Medical Association* no. 281 (1999): 2127–2137.
- Hentoff, Nat. "The FBI's Magic Lantern." *Village Voice*. 47, no. 22 (June 4, 2002): p. 35.
- Herschensohn, Bruce. "What Proof? Terrorism Alone Is Cause for Action." *Los Angeles Times*. (October 5, 2001): B15.
- Hershberg, James G. "Soviet Archives: The Opening Door." *Cold War International History Project Bulletin* 1 (Spring 1992): 1, 12.
- Herskovitz, Don. "A Sampling of Direction-Finding Systems." *Journal of Electronic Defense* 23, no. 8 (August 2000): 57–65.
- Hessman, James D. "The Maritime Dimension; Special Report: The Coast Guard's Role in Homeland Defense." *Sea Power* (Apr 2002), pp. 26–30.
- Heywood, Karen J. "Fluid Flows in the Environment: An Introduction." *Physics Education*. 28 (1993): 43.
- Hiatt, Mark. "Computers and the Revolution in Radiology." *Journal of the American Medical Association*. (April 5, 1995): 1062.
- Hickey, Neil. "So Big: The Telecommunications Act at Year One." *Columbia Journalism Review* Jan/Feb. 1997: 23–28.
- Higgins, Thomas V. "Technologies Merge to Create High-Density Data Storage." *Laser Focus World* (August 1993): 57–65.
- Hirsch, Daniel. "The NRC: What, Me Worry?" *Bulletin of the Atomic Scientists* 58, no. 1 (January/February 2002): 38–44.
- Hirsch, Michael. "Bush and the World." *Foreign Affairs* 81, no. 5 (September/October 2002): 18–44.
- Hoagland, Jim. "CIA's New Old Iraq File." *Washington Post*. (October 20, 2002): B7.
- Hoffman, Bruce. "Is Europe Soft on Terrorism?" *Foreign Policy* no. 115 (Summer 1999): 62–76.
- Hogan, William J. "Energy from Inertial Fusion." *Physics Today* September 1992, pp. 42–50.
- Hogue, Cheryl. "Regulators at Scene of Attacks." *Chemical & Engineering News* 79, no. 39 (September 24, 2001): 11.
- Hollister, Anne. "Blimps." *Life Magazine*. 4 (1988): 65–69.
- Holzer, T.L., J.B. Fletcher, G.S. Fuis, T. Ryberg, T.M. Brocher, and C.M. Dietel. "Seismograms Offer Insight into Oklahoma City Bombing." *Eos, Transactions American Geophysical Union*, vol. 77, no. 41 (October 8, 1996): 393, 396–397.
- "Homeland Security Dept.: Is \$36.2 Billion Enough?" *Aviation Week & Space Technology* 158, no. 7 (February 17, 2003): 57–58.
- Horn, M.K. "Oil and Gas." *Geotimes*, vol. 40, no. 2, 1995.
- Hosenball, Mark, and Greg Vistica. "The Search for Clues: Did Officials Miss Hints of an Impending Attack?" *Newsweek*. November 6, 2000:45.
- House Committee on Foreign Affairs. *U.S. Policy in the Aftermath of the Bombing of Pan Am 103*. Hearing before the Subcommittees on International Security, International Organizations, and Human Rights. 103rd Cong., 2nd sess., July 28, 1994.
- Houston, Betsy. "Science and Technology Is Prominent in the Department of Homeland Security." *JOM* 55, no. 1 (January 2003): 9.

- "How Secure Are Your Phone, Fax, Data Transmission Systems?" *Security* 34, no. 6 (June 1997): 75–76.
- Huband, Mark. "U.S. Rejected Sudanese Files on al-Qaeda." *Financial Times*. (November 30, 2001): 1.
- Hughes, David. "Homeland Security Dept.: So Many Details, So Little Time." *Aviation Week & Space Technology* 157, no. 23 (December 2, 2002): 71.
- Hughes, David. "New Westinghouse Airship Designed for Early Warning Surveillance." *Aviation Week & Space Technology* 135 (1991): 24–25.
- Huleatt, Richard S. "Computer Supersnoop: The New Department of Homeland Security." *Information Intelligence Online Newsletter* 23, no. 12 (December 2002): 2–4.
- Huleatt, Richard S. "EPIC May Never Learn Details of Government Keystroke Monitor." *Information Intelligence Online Newsletter* 22, no. 10 (October 2001): 5–6.
- Hunter, David H. "The Evolution of Literature on United States Intelligence." *Armed Forces and Society* 5, no. 1 (1978): 31–52.
- "IACP's Less Lethal Force Options Course." *Law & Order* 49, no. 9 (September 2001): 95–99.
- Inchniowski, Tom. "Ridge Will Face Big Challenges as Homeland Security Leader." *ENR* 250, no. 3 (January 27, 2003): 9.
- Inglesby, T.V., et al. "Anthrax as a Biological Weapon." *Journal of the American Medical Association* no. 281 (May 1999): 1735–1745.
- Ingram, Gregory. "Roundtable Discussion: Critical Issues in Infrastructure in Developing Countries." *Work Bank Research Observer* (1993): 473.
- Ingram, Judith. "Russia Accuses U.S. of Espionage." *Chicago Sun-Times*. (April 11, 2002): 27.
- International Genome Sequencing Consortium, "Initial Sequencing and Analysis of the Human Genome." *Nature* 409 (2001): 860–921.
- Jackman, Tom. "Retiree Surrenders in 1975 Va. Killing." *Washington Post*. (May 22, 2002): B7.
- Jackman, Tom. "Terror Suspect Allowed to Seek Foreign Aid." *Washington Post*. (July 18, 2002): B2.
- Jackson, Robert L. "Sessions Concedes FBI Erred in Central American Activist Probe." *Los Angeles Times*. (February 3, 1988): 16.
- Jankovic, Joseph, and Mitchell F. Brin. "The Therapeutic Uses of Botulinum Toxin." *New England Journal of Medicine* 324 (25 April 1991): 1186.
- Jarvis, Ray. "Robot Navigation." *The Industrial Robot* 21, no. 2 (1994): 3.
- Jayaramen, K. S. "Indian Plague Poses Enigma to Researchers." *Nature* (13 October 1994): 547.
- Jeffereys, A.J. "Hypervariable 'minisatellite' Regions in Human DNA." *Nature* no. 314 (1987): 67–73.
- Jeffers, B. R. "Human Biological Materials in Research: Ethical Issues and the Role of Stewardship in Minimizing Research Risks." *Advances in Nursing Science* no. 24(2) (2001): 32–46.
- Jeffords, J.M., and Tom Daschle. "Political Issues in the Genome Era." *Science* 291 (16 February 2001): 1249–50.
- Jeffrey, Terence P. "Two Silicon Valley Engineers Indicted for Economic Espionage Aiding China." *Human Events* 59, no. 2 (January 13, 2003): 1.
- Jeffreys-Jones, Rhodri. "Review Article: Manual Indices and Digital Pathways: Developments in United States Intelligence Bibliography." *Intelligence and National Security* 9, no. 3 (Jul. 1994): 555–559.
- Jeffreys-Jones, Rhodri. "The Historiography of the CIA." *Historical Journal* 23 (Jun. 1980): 489–496.
- Jenkins, Sally. "Peaceful Games, Cold War Sentiment." *Washington Post*. (February 25, 2002): D1.
- Jensen, Torkil H. "Fusion-A Potential Power Source." *Journal of Chemical Education*, October 1994, pp. 820–823.
- Jernigan, J.A., D.S. Stevens, D.A. Ashford, et al. "Bioterrorism-Related Inhalational Anthrax: The First 10 Cases Reported in the United States." *Emerging Infectious Diseases* no. 7 (2001).
- Jezeq, Z. "20 Years Without Smallpox." *Epidemiology, Microbiology, and Immunology* 49, no. 3 (2000): 95–102.
- Johnson, George. "The Spies' Code and How It Broke." *New York Times, Week in Review*. July 16, 1995.
- Johnson, Jeff. "Truckers, Shippers Blast Customs Security Plan." *Transport Topics* no. 3521 (January 27, 2003): 1.
- Johnson, Jeff. "Unclear Future at Weapons Labs." *Chemical & Engineering News* 78, no. 49 (December 4, 2000): 51–58.
- Johnson, K., and R. Willing. "Ex-CIA Chief Revitalizes 'truth serum' Debate." *USA Today*. (April 26, 2002): 12a.
- Johnson, Kevin. "Recruits Flood Federal 'Boot Camp'." *USA Today*. (September 23, 2002): A3.
- Johnston, David. "F.B.I. Warns Local Agencies to Be Aware." *New York Times*. (September 10, 2002): A17.
- Johnston, David. "FBI Director Rejects Agency for Intelligence in United States." *New York Times*. (December 20, 2002): A22.
- Johnston, David. "Strength Is Seen in a U.S. Export: Law Enforcement." *New York Times*. (April 17, 1995): A1.
- Johnson, J. L., and Jaime R. Taylor. "Image Factorization: A New Hierarchical Decomposition Technique." *Optical Engineering*, vol. 38 (Sept 1999): 1517–23.
- Johnson, J. L., M. L. Padgett, and O. Omidvar, "Overview of Pulse Coupled Neural Networks (PCNN)." *IEEE Transactions on Neural Networks*, vol. 10, Special Issue 3 (1999): 461–63.
- Jones, Jerry W. "CI and HUMINT or HUMINT and CI or CI/HUMINT or TAC HUMINT (Confusing, Isn't It?)" *Military Intelligence Professional Bulletin* 28, no. 2 (April-June 2002): 28–33.
- Joyce, Jim. "Espionage Battleground." *Security* 40, no. 1 (January 2003): 24–25.
- Kahn, A.S., S. Morse, and S. Lillibridge. "Public-Health Preparedness for Biological Terrorism in the USA." *Lancet* no. 356 (2000): 1179–1182.
- Kaltenhauser, Skip. "Industrial Espionage Is Alive and Well." *World Trade* 10, no. 7 (July 1997): 24–26.
- Kaplan, David E., Chitra Ragavan, Richard J. Newman, et al. "Terror's Grim Toll." *U.S. News & World Report*. October 30, 2000:32.
- Karmon, Ely. "Counterterrorism Policy: Why Tehran Stops and Starts Terrorism." *Middle East Quarterly*, vol. 5, no. 4 (December 1998).
- Kaufmann, A.F., M.I. Meltzer, and G.P. Schmid. "The Economic Impact of a Bioterrorist Attack: Are Prevention and Postattack

- Intervention Program Justifiable?" *Emerging Infectious Diseases* no. 3 (1997): 83–94.
- Kedzierski, Marie. "Vaccines and Immunization (sic)." *New Scientist* 133 (8 February 1992): S1.
- Kent, Cheryl. "A Safer Federal Building for Oklahoma City." *New York Times*. (August 22, 1999): 34.
- Khor, Jennifer. "Information Gathering, the Law of War, and Peacekeeping." *Peacekeeping & International Relations* 24, no. 6 (November 1995): 16.
- Khoury, M.J., L.L. McCabe, and E.R.B. McCabe. "Genomic Medicine: Population Screening in the Age of Genomic Medicine." *The New England Journal of Medicine* no. 348(1) (2003): 50–58.
- Kilian, Michael. "Patriot Missile Miscalculations a Cause for U.S. Concern." *Chicago Tribune*. (March 27, 2003): 5.
- Killian, Michael. "New Defensive Posture for Former Prosecutor: Threat from Sea a Top Priority." *Chicago Tribune*. (February 13, 2002): 7.
- Kirkpatrick, Melanie. "Weapons with a Moral Dimension." *Wall Street Journal*. (January 14, 2003): A15.
- Knight, Amy. "Russian Archives: Opportunities and Obstacles." *International Journal of Intelligence and Counterintelligence* 12, no. 3 (Fall 1999): 325–337.
- Koper, K.D., T.C. Wallace, S.R. Taylor, and H.E. Hartse. "Forensic Seismology and the Sinking of the Kursk." *Eos, Transactions, American Geophysical Union*, vol. 82, no. 4 (2001): 37.
- Koster, J.E., et al. "Alpha Detection as a Probe for Counter Proliferation." *28th Annual International Carnahan Conference on Security Technology(IEEE)*. (October 1994):6–19.
- Kowalski, W.J., W.P. Bahnfleth, and T.S. Whittam., "Filtration of Airborne Microorganisms: Modeling and Prediction." *ASHRAE Transactions* 105 (1999): 4–17.
- Kreuzer, Heidi. "Westchester Incident Highlights Oil Spill Concerns." *Pollution Engineering* 33, no. 1 (January 2001): 9–10.
- Kruse, V. J., et al. "Impacts of a Nominal Nuclear Electromagnetic Pulse on Electric Power Systems: A Probabilistic Approach." *IEEE Transactions on Power Delivery*, vol. 6, No. 3, July 1991: 1251–1263.
- Ksiazek T.G., et al. "A Novel Coronavirus Associated with Severe Acute Respiratory Syndrome." *New England Journal of Medicine* 10.1056 (April 10, 2003): a030781.
- Kupperschmid, David. "James Bond 'Supplier' Has the Cure for Whatever Is Bugging You." *Los Angeles Times*. (April 26, 1985): 2.
- Kushner, Harvey W. "Can Security Measures Stop Terrorism?" *Security Management* 40, no. 6 (June 1996): 132.
- Kuzio, Taras. "Details Emerge on Kiev's 'Alpha' Unit." *Jane's Intelligence Review* 11, no. 10 (October 1, 1999): 1.
- Lacy, D.B., W. Tepp, A.C. Cohen, et al. "Crystal Structure of Botulinum Neurotoxin Type A and Implications for Toxicity." *Nature Structural Biology* no. 5 (1998): 898–902.
- Ladika, Susan. "Tracing the Shadowy Origins of Nuclear Contraband." *Science* no. 5522 (2001): 1634.
- Landers, Jay. "Safeguarding Water Utilities." *Civil Engineering* 72, no. 6 (June 2002): 48–53.
- Lang, John. "CIA Ads Tout Career in Espionage." *Dallas Morning News*. (November 1, 1998): 15A.
- Lardner, George, Jr. "Classified Trial-Data Law Attacked." *Washington Post*. (April 30, 1988): A4.
- Lardner, George, Jr. "Panel Proposes Tougher Laws Against Espionage." *Washington Post*. (May 24, 1990): A16.
- Lardner, Richard. "Keeping Secrets." *Government Executive* 30, no. 3 (March 1998): 27–29.
- Lardner, Richard. "The Need to Know." *Government Executive* 29, no. 2 (February 1997): 16–21.
- Larson, Virgil. "The Next Wave: Using Radio Frequency as a Weapon." *Omaha World-Herald*. (April 14, 2002): 1D.
- Lawler, Andrew. "Rules Eased on Satellite Projects." *Science* 296, no. 5566 (April 12, 2002): 237–238.
- Leader, Stefan. "Cash for Carnage: Funding the Modern Terrorist." *Jane's Intelligence Review* (May 1, 1998): 36.
- Leary, Warren E. "Test of Revolutionary Jet Promises to Transform Flight." *New York Times*. (May 22, 2001): F4.
- LeDuc, J.W., I. Damar, J.M. Meegan, et al. "Smallpox Research Activities: U.S. Interagency Collaboration 2001." *Emerging and Infectious Diseases* 8 (2002): 743–745.
- Lee, Christopher, and Sara Kehaulani Goo. "TSA Blocks Attempts to Unionize Screeners." *Washington Post*. (January 10, 2003): A19.
- Lee, Christopher. "Agencies Fail Cyber Test; Report Notes 'Significant Weaknesses' in Computer Security." *Washington Post*. (November 20, 2002): A23.
- Lee, Jennifer. "Guerilla Warfare, Waged with Code." *New York Times*. October 10, 2002.
- Lehman, John. "Silent, Deep, Deadly." *Wall Street Journal*. (November 11, 1998): 1.
- Leonard, Raymond W. "Studying the Kremlin's Secret Soldiers: A Historiographical Essay on the GRU, 1918–1945." *Journal of Military History* (Jul. 1992): 403–421.
- Lester, Andrew J, and Clifton L. Smith. "Analyses of Performance of Volumetric Intrusion Detection Technologies." *Proceedings, 33rd Annual International Carnahan Conference on Security Technology*. (October 1999): 101–111–58.
- "Let's Have Straight Talk on Missile Defenses." *Aviation Week & Space Technology* 145, no. 16 (October 14, 1996): 86.
- Leung, W.C. "The Prosecutor's Fallacy—A Pitfall in Interpreting Probabilities in Forensic Evidence." *Med Sci Law*. 1.(2002):44–50.
- Levine, Bernard. "What's Next for Electronics?" *Electronic News* 47, no. 40 (October 1, 2001): 1.
- Lewis, George N., and Theodore A. Postol. "Future Challenges to Ballistic-Missile Defense." *IEEE Spectrum*, (September, 1997): 6–68.
- Li Shaomin. "My Long Journey Home." *Wall Street Journal*. (August 7, 2001): A14.
- Lichtblau, Eric. "FBI and CIA to Move Their Counterterror Units to a Single New Location." *New York Times*. (February 15, 2003): A14.
- Lichtblau, Eric. "White House Report Stings Drug Agency on Abilities." *New York Times*. (February 5, 2003): A16.
- Litke, Alan M., and Andreas S. Schwarz. "The Silicon Microstrip Detector." *Scientific American*. (May, 1995): 76.

- Lombardi, Gianni. "The Contribution of Forensic Geology and Other Trace Evidence Analysis to the Investigation of the Killing of Italian Prime Minister Aldo Moro." *Journal of Forensic Sciences*, vol. 44, no. 3 (1999): 634–642.
- Lombardi, Kate Stone. "Air Travel Under a More Watchful Eye." *New York Times*. (January 26, 2003): WC1.
- "Looking Glass Gets a Rest at Last." *Chicago Tribune*. (July 29, 1990): 2.
- Lowenthal, Mark M. "The Intelligence Library: Quantity vs. Quality." *Intelligence and National Security* 2, no. 2 (Apr. 1987): 368–373.
- "Low-Power FM Transmitters." *Electronics Now* 70, no. 8 (August 1999): 37–40.
- Lucia, Christine. "Counterproliferation at Core of New Security Strategy." *Arms Control Today* 32, no. 8 (October 2002): 30.
- Lukasik, S. J., J. T. Goldberg, and S. E. Goodman. "Protecting an Invaluable and Ever-Widening Infrastructure." *Association for Computing Machinery* 41, no. 6 (June 1998): 11–16.
- Macintyre, A.G., C.G.W. Eitzen, Jr., R. Gum, et al. "Weapons of Mass Destruction Events with Contaminated Casualties: Effective Planning for Health Care Facilities." *Journal of the American Medical Association* no. 283 (2000): 252–253.
- MacLeod, Scott, Elaine Shannon, Mark Thompson, Edward Barnes, and William Dowell. "How Feuds and Culture Clashes have Stymied the USS *Cole* Investigation." *Time*. vol. 158 (July 16, 2001):38.
- MacSweeney, Greg. "Caller ID with a Kick." *Insurance & Technology* 25, no. 10 (October 2000): 30–35.
- Mallet, Victor. "Pretoria Faces German Bugging Protest." *Financial Times*. (November 22, 1999): 10.
- Marashi, Ibrahim al-. "Iraq's Security and Intelligence Network: A Guide and Analysis." *Middle East Review of International Affairs*. 6:3 (September, 2002).
- Marcus, David L. "Horror at U.S. Embassies." *Boston Globe*. (August 8, 1998): A1.
- Markoff, John, and John Schwartz. "Bush Administration to Propose System for Monitoring Internet." *New York Times*. December 20, 2002.
- Markoff, John. "British Concern to Help U.S. Track Terrorists." *New York Times*. (October 12, 2002): A8.
- Marquand, Robert. "As War Looms, U.S. Talks to China." *Christian Science Monitor*. (October 21, 2002): 6.
- Marquis, Christopher. "Some Lawmakers Urging U.S. to Speed Exports of Satellites." *New York Times*. (July 9, 2001): A7.
- Marshall, Eliot. "Patriot's Scud Busting Record is Challenged." *Science* 252, no. 5006 (May 3, 1991): 640–641.
- Marsili, Ray. "New Techniques Revolutionize Analyses of Liquid Samples." *Research & Development* 42, no. 2 (February 2000): 22–24.
- Matthews, William. "Energy Agency Says Web Info Poses Threat." *Federal Computer Week* 16, no. 34 (September 23, 2002): 46.
- Maurer, H.H. "Liquid Chromatography-Mass Spectrometry in Forensic and Clinical Toxicology." *J Chromatogr B Biomed Sci Appl*. 713 (1998): 3–25.
- McCarter, Kimberly M. "Tape Recording Interviews." *Marketing Research* 8, no. 3 (fall 1996): 50–51.
- McConnell, Bruce. "Telecom Role Model." *Federal Computer Week* 16, no. 40 (November 11, 2002): 27.
- McCullagh, Declan. "FBI Agents Soon May Be Able to Spy on Internet Users Legally Without a Court Order." *New York Times*. (September 14, 2001.)
- McManus, Doyle. "A U.S. License to Kill." *Los Angeles Times*. (January 11, 2003): A1.
- McPhee, John. "Annals of Crime—The Gravel Page." *The New Yorker*. (January 29, 1996): 44–69.
- Mehta, Stephanie N. "Playing Hide-and-Seek by Telephone—Phone Companies Are Arming Both Sides in the Battle to Screen Unwanted Callers." *Wall Street Journal*. (December 13, 1999): B1.
- Melloan, George. "Civil Liberties Give Way to the Search for Terrorists." *Wall Street Journal*. (October 23, 2001): A27.
- Melton, R. H. "Panel Criticizes U.S. Anti-Terrorism Preparedness." *Washington Post*. (December 16, 1999): A6.
- Meyer, Josh. "At Least 70,000 Terrorist Suspects on Watch List." *Los Angeles Times*. (September 22, 2002): A1.
- Milbank, Dana, and T. R. Reid. "New Global Threat Revives Old Alliance." *Washington Post*. (October 16, 2001): A10.
- "Military Launches New EW Efforts." *Aviation Week & Space Technology* 157, no. 19 (November 4, 2002): 35–43.
- "Military Operations Named." *Marine Corps Gazette* 85, no. 11 (November 2001): 4.
- Miller, Bill. "National Alert System Defines Five Shades of Terrorist Threat." *Washington Post*. (March 13, 2002): A15.
- Miller, Leslie. "Some Airport Screeners Raise Rates." *San Diego Union-Tribune*. (August 27, 2002): A7.
- Mintz, John, and Spencer Hsu. "Customs Takes over Monitoring Local Skies." *Washington Post*. (January 28, 2003): A6.
- Mintz, John. "15 Freighters Believed to Be Linked to al Qaeda." *Washington Post*. (December 31, 2002): A1.
- Mintz, John. "Fearing Attack by Sea, U.S. Tracking 'Ships of Concern.'" *Seattle Times*. (December 31, 2002): A1.
- Mitchell, Russ, Richard Folkers, and Susan Gregory. "Why Melissa Is So Scary." *U.S. News & World Report* (April 12, 1999): 34–36.
- Molloy, Thomas. "Why Some In-Country English Language Programs Do Not Work." *DISAM: Journal of International Security Assistance Management* 24, no. 4 (summer 2002): 125–130.
- Montecucco, C. (ed.). "Clostridial neurotoxins: the molecular pathogenesis of tetanus and botulism." *Current Topics in Microbiology and Immunology* no. 195 (1995): 1–278.
- "Months After Anthrax Scare, Mail-Safety Goals are Unmet." *USA Today*. (August 29, 2002): 12a.
- Mooney, Chris. "Spy Tech." *The American Prospect* 13, no. 2 (January 28, 2002): 39–41.
- Morais, Herbert V. "The War Against Money Laundering, Terrorism, and the Financing of Terrorism." *Lawasia Journal* (2002): 1–32.
- Morris, Jim. "Israel Offers Lessons in Aviation Security." *Dallas Morning News*. November 8, 2001.
- "Moscow, Tehran to Discuss RF Weapons Supplies to Iran—VP." *Itar-Tass News Wire*. (February 28, 2001): 1.



- Muhlebach, Richard. "What's Your Disaster Plan?" *National Real Estate Investor* 44, no. 8 (August 2002): 64.
- Mulkern, Anne C. "Agency Tackles National Security: NIST's Boulder Lab Developing Technologies to Combat Terrorism." *Denver Post*. (January 25, 2002): C1.
- Mullis, K.B. and F.A. Faloona. "Specific synthesis of DNA In Vitro Via a Polymerase Catalysed Chain Reaction." *Methods in Enzymology* no. 155 (1987): 335–350.
- Munro, N.B., S.S. Talmage, G.D. Griffin, et al. "The Sources, Fate, and Toxicity of Chemical Warfare Agent Degradation Products." *Environmental Health Perspectives* no. 107 (1999): 933–974.
- Munro, Neil. "Fighting for Intelligence Funds." *Washington Technology* (July 27, 1995): 1.
- Muradian, Vago. "Better Export Controls Needed to Check Dual-Use Technologies." *Defense Daily* 198, no. 14 (January 22, 1998): 1.
- Murphy, Dean E. "As Security Cameras Sprout, Someone's Always Watching." *New York Times*. (September 29, 2002).
- Myers, Steven Lee. "U.S. 'Updates' All-Out Atom War Guidelines." *New York Times*. (December 8, 1997): A3.
- Nahum, Hazi, and Sheike Marom. "Aerostat-Borne Systems for Defense and Homeland Security." *Military Technology* 26, no. 8 (August 2002): 102–108.
- Nakajima, T., S. Ohta, Y. Fukushima, et al. "Sequelae of Sarin Toxicity at One and Three Years After Exposure in Matsumoto, Japan." *Journal of Epidemiology* no. 9 (1999): 337–343.
- Nakamura, Y., M. Leppert, P. O'Connell, et al. "Variable Number Tandem Repeat (VNTR) Markers for Human Gene Mapping." *Science* no. 237 (1987): 1616–1622.
- Nasheri, Hedieh, and Timothy J. O'Hearn. "High-Tech Crimes and the American Economic Machine." *International Review of Law, Computers & Technology* 13, no. 1 (March 1999): 7–19.
- National Drug Intelligence Center, United States Department of Justice. *National Drug Threat Assessment 2001: The Domestic Perspective* Johnstown, PA: National Drug Intelligence Center, October 2000.
- Nelson, Scott Bernard. "U.S. Offers \$5M in Financial War on Terrorism." *Boston Globe*. (November 14, 2002): C1.
- "The New Department of Homeland Security." *Chemical Engineering Progress* 99, no. 2 (February 2003): 25.
- "New Guidelines Offered for Emergency Response Plans." *Environmental Management Today* 7, no. 3 (July/August 1996): 5.
- Newman, William W. "Reorganizing for National Security and Homeland Security." *Public Administration Review* 62 (September 2002): 126–137.
- Ng Ken Boon. "Enabling Net Connection Sharing." *InternetWeek* no. 872 (August 6, 2001): 1.
- "NIJ Technologies for Public Safety." *Law & Order* 50, no. 8 (August 2002).
- "NIPC Loses One of Its Own to 'Beltway' Sniper." *Computerworld* 36, no. 43 (October 21, 2002): 6.
- Noguchi, Yuki. "'Star Trek' Tech Gets Limited Approval." *Washington Post*. (February 15, 2002): E1.
- Nolte, Carl. "Spy Store a Boon for Paranoid Public." *San Francisco Chronicle*. (January 18, 2002): A23.
- Nordland, Rod; John Barry, Mark Hosenball, Debra Rosenberg, and Gregory Vistica. "A Sneak Attack: Death at Sea" *Newsweek*. October 23, 2000: 27.
- "Novel Design of Countermine Robot." *Jane's International Defense Review* (February 1, 1996): 20.
- Nowlan, W. "A Rational View of Insurance and Genetic Discrimination." *Science* no. 297(5579) (2002): 195–196.
- "Nuclear Security Gets First Director: Gordon Confirmed as GOP Blasts His Boss, Richardson." *Washington Post*. (June 15, 2000): A31.
- Nye, Joseph S., Jr. "Peering into the Future." *Foreign Affairs* 73, no. 4 (July/August 1994): 82.
- Oldham, Scott. "Less-Lethal Munitions." *Law & Order* 50, no. 2 (September 2002): 54–56.
- Olson, James M. "The Ten Commandments of Counterintelligence." *Studies in Intelligence* no. 11 (fall-winter 2001).
- Olson, Tod. "America Held Hostage: The Iranian Hostage Crisis Would Torment America and Topple a President." *Scholastic Update*, vol. 130 (May 11, 1998): 20–22.
- "ONDCP Says Anti-Drug Ads Are Ineffective." *Crime Control Digest* 36, no. 20 (May 17, 2002): 4.
- Opderbecke, J. "Depth Image Matching for Underwater Vehicle Navigation." *Image Processing*, vol. 2 (1999): 624–629.
- O'Toole, T. "Smallpox: An Attack Scenario." *Emerging Infectious Diseases* 5 (1999): 540–546.
- Ottaway, David B. "Reagan Building Vulnerable to Attack." *Washington Post*. (March 8, 1999): A1.
- Pake, George E. "Nuclear Magnetic Resonance in Bulk Matter." *Physics Today* (October 1993): 46.
- Palfrey, Terry. "The Hidden Legacy of Scott: Weapons of Mass Destruction and the UK Government Proposals to Control the Transfer of Technology by Intangible Means." *International Review of Law, Computers & Technology* 13, no. 2 (August 1999): 163–181.
- Park, S.J, T.A. Taton, and C.A. Mirkin. "Array-Based Electrical Detection of DNA with Nanoparticle Probes." *Science* no. 5559 (2002): 1503–1506.
- Pasternak, D. "Wonder Weapons." *U.S. News & World Report*. July 7 (1997): 38–46.
- Peake, Hayden B. "SIGINT Literature: World War I to the Present." *American Intelligence Journal* 15, no. 1 (Spring/Summer 1994): 88–92.
- Perera, F.P., and I.B. Weinstein. "Molecular Epidemiology: Recent Advances and Future Directions." *Carcinogenesis* 21 (2000): 517–524.
- Perry, R.D., and J.D. Fetherston. "Yersinia Pestis-Etiological Agent of Plague." *Clinical Reviews in Microbiology* no. 10 (January 1997): 35–66.
- Peters, C.J., and J.W. LeDuc. "An Introduction to Ebola: The Virus and the Disease." *The Journal of Infectious Diseases* no. 179 (Supplement 1, February 1999): ix–xvi.
- Peters, Katherine McIntire. "Lost in Translation." *Government Executive* 34, no. 5 (May 2002): 39–45.
- Phillips, Edward H. "It Wasn't Us." *Aviation Week & Space Technology* 144, no. 15 (April 8, 1996): 19.

- Phillips, Edward H. "USAF Testing CV-22 Countermeasures." *Aviation Week & Space Technology* 157, no. 15 (October 7, 2002): 59.
- Piazza, Peter. "Sunset of the CIA? Industry May Decide." *Security Management* 44, no. 11 (November 2000): 36.
- Piazza, Peter. "Tools for Digital Sleuths." *Security Management* 46, no. 4 (April 2002): 36.
- Pincus, Walter, and Mike Allen. "Terrorism Agency Planned: Center to Integrate Intelligence, Analysis." *Washington Post*. (January 29, 2003): A12.
- Pincus, Walter. "CIA, Pentagon Back NIMA 'Concept,' Combining Spy Satellite Photo Units." *Washington Post*. (November 29, 1995): A23.
- Pincus, Walter. "Computer Shutdown Hits Defense Security Service; Backlog of Background Checks Grows." *Washington Post*. (July 8, 2000): A10.
- Pincus, Walter. "DOE Plan Riles Senate GOP: Choice of Richardson to Run New Bomb Agency Spurs Pay Threat." *Washington Post*. (October 19, 1999): A17.
- Plotkin, Stanley A. "Vaccination in the 21st Century." *The Journal of Infectious Diseases*, vol. 168 (1993): 29–37.
- Poole, Patrick. "'Echelon' Spells Trouble for Global Communications." *Privacy Journal* 25, no. 11 (September 1999): 3–4.
- Porch, Douglas. "French Intelligence Culture: A Historical and Political Perspective." *Intelligence and National Security* 10, no. 3 (July 1995): 486–511.
- Postel, Sandra L., and Aaron T. Wolf. "Dehydrating Conflict." *Foreign Policy* no. 126 (September/October 2001): 60–67.
- Pound, Edward T. "Keeping Secrets Secret." *U.S. News & World Report*. (June 3, 2002): 22.
- Pound, Edward T. "Security Panel Has Opposed Agency's Cost-Cutting Moves." *USA Today*. (August 20, 1999): 8A.
- Prados, John. "Understanding Central Intelligence." *Bulletin of the Atomic Scientists* 58, no. 2 (March/April 2002): 64–65.
- Price, Thomas J. "Spy Stories: Espionage and the Public in the Twentieth Century." *Journal of Popular Culture* no. 30 (1996): 81–89.
- Priest, Dana, and Juliet Eilperin. "Panel Finds No 'Smoking Gun' in Probe of 9/11 Intelligence Failures." *Washington Post*. (July 11, 2002): A1.
- Prince, Paul. "Static Electricity." *Tele.com* 6, no. 17 (September 3, 2001): 28.
- Quist, D., and I.H. Chapela. "Transgenic DNA Introgressed Into Traditional Maize Landraces in Oaxaca, Mexico." *Nature* no. 414 (2001): 541–3.
- Raber, E. "L-Gel Decontaminates Better Than Bleach." *Science and Technology Review*, March (2002): 10–16.
- "Race to Pick a Better Cipher." *Science* no. 5382 (1998): 1411.
- "RAMPART Assesses Threats." *Signal* 56, no. 1 (September 2001): 7.
- Rappert, Brian. "Assessing Technologies of Political Control." *Journal of Peace Research* 36, no. 6 (November 1999): 741–750.
- Reddy, Anitha. "Terrorists Are Now Targets in Money-Laundering Fight." *Washington Post*. (July 25, 2002): E3.
- Reeves, A. "Tracing Biothreats with Molecular Signatures." *Los Alamos National Laboratory Research Quarterly*, Fall 2002: 15–17.
- Reiss, Tom. "Now Will We Heed the Biological Threat?" *New York Times*. (February 21, 1998): 11.
- "Remarks on Signing the Intelligence Authorization Act for Fiscal Year 2003." *Weekly Compilation of Presidential Documents* 38, no. 48 (December 2, 2002): 2101–2102.
- "Reports Shed Light on World Trade Center Collapses, Look to Safer Structures in the Future." *JOM* 54, no. 6 (June 2002): 6.
- Reppert, Barton. "Training the Tongue-Tied." *Government Executive* 34, no. 4 (April 2002): 66.
- "Responses to ASR's Survey on Aviation Security Post-Sept. 11." *Airport Security Report* 9, no. 19 (September 11, 2002): 1.
- Revelle, Daniel J., and Lora Lumpe. "Third World Submarines." *Scientific American*. (August 1994): 16–21.
- Rhodes, Keith A. "USPS Air Filtration Systems Need More Testing and Cost Benefit Analysis Before Implementation." *FDCH Government Account Reports* (August 22, 2002).
- Rice, Condoleeza. "Anticipatory Defense in the War on Terror." *New Perspectives Quarterly* 19, no. 4 (fall 2002): 5–8.
- Richardson, T. "Pitfalls in Forensic Toxicology." *Ann Clin Biochem*. 37 (2000): 20–44.
- Ritchie-Matsumoto, Peggy. "Taking Your Technology to the Marketplace." *Corrections Today* 62, no. 4 (July 2000): 96–100.
- Rivers, Brendan. "U.S. Navy Orders OUTBOARD Update." *Journal of Electronic Defense* 23, no. 8 (August 2000): 31.
- Rivkin, David B., Jr. "The Laws of War." *Wall Street Journal*. (March 4, 2003): A14.
- Robbins, J., and A.B. Schneider. "Thyroid Cancer following Exposure to Radioactive Iodine." *Reviews in Endocrine and Metabolic Disorders* no. 1 (2000): 197–203.
- Robinson, C. Paul, Joan B. Woodward, and Samuel G. Varnado. "Critical Infrastructure: Interlinked and Vulnerable." *Issues in Science and Technology* 15, no. 1 (fall 1998): 61–67.
- Robinson, Clarence O, Jr. "Position-Fixing Methods Use Broadband Direction Finders." *Signal* 53, no. 2 (October 1998): 71–74.
- "Robo, P.I." *American Scientist* 90, no. 1 (January/February 2002): 28–29.
- Romanko, J. R. "Truth Extraction." *New York Times Magazine*. (November 19, 2000): 54.
- Romano, Jay. "Terrorism Insurance, at a Price." *New York Times*. (March 9, 2003): 5.
- Rosenbarger, Matt. "Less-Lethal Improvements: Federal and ALS Work Together." *Law & Order* 49, no. 11 (November 2001): 84–86.
- Rosenthal, E. "From China's Provinces, a Crafty Germ Spreads." *New York Times*. (April 27, 2003).
- Rosenthal, S.R., M. Merchlinsky, C. Kleppinger, et al. "Developing New Smallpox Vaccines." *Emerging Infectious Diseases* no. 7 (2001): 920–926.
- Rothenberg, K.H., and S.F. Terry. "Before It's Too Late—Addressing Fear of Genetic Information." *Science* no. 297(5579) (2002): 196–197.

- Rubin, Debra K. "FEMA and Corps Plan New Guide for Terrorism Catastrophes." *ENR* 249, no. 15 (October 7, 2002): 14.
- "Russia Developing New Radio Frequency Weapons." *Electromagnetic News Report* 30, no. 2 (March/April 2002): 1.
- "S. 1447, Aviation and Transportation Security Act." *Airports* 18, no. 48 (November 27, 2001): 5.
- Safire, William. "China Syndrome: Clinton's Greed for Funds Triggers a Security Meltdown." *New York Times*. (May 18, 1998): A19.
- Safire, William. "Whitewash at Justice." *New York Times*. (July 16, 1999): A19.
- Salamon, Julie. "A Detective-Story Approach to the Twin Towers' Collapse." *New York Times*. (April 30, 2002): E1.
- Samii, Abbas William. "The Shah's Lebanon Policy: The Role of SAVAK." *Middle Eastern Studies* 33, no. 1 (January 1997): 66–91.
- Sample, Ian. "Just a Normal Town." *New Scientist* 167, no. 2245 (July 1, 2000): 20.
- Schaumburg, Ron. "Americans Held Hostage." *New York Times Upfront*. vol. 133(January 15, 2001): 23.
- Schmemmann, Serge. "Soviet Archives Provide Missing Pieces of History's Puzzles." *New York Times*. (Feb. 8, 1993).
- Schmemmann, Serge. "Soviet Archives: Half-Open, Dirty Windows on Past." *New York Times*. (Apr. 4, 1995).
- Schmidt, Susan. "DEA to Bolster Presence Along Mexican Border, in Central Asia." *Washington Post*. (August 10, 2002): A11.
- Schmitt, C.K., K.C. Meysick, and A.D. O'Brien. "Bacterial Toxins: Friends or Foes?" *Emerging Infectious Diseases* no. 5 (1999): 224–234.
- Schneider, Greg, and Sara Kehaulani Goo. "For Air Marshals, a Steep Takeoff." *Washington Post*. (January 2, 2003): A1.
- Schneider, Greg. "No Whistleblowing Protections for Airport Baggage Screeners." *Washington Post*. (February 8, 2002): A29.
- Schneider, Howard. "A Little U.S. Pop-aganda for Arabs." *Washington Post*. (July 26, 2002): A24.
- Schneider, Howard. "Syria Evolves as Anti-Terror Ally." *Washington Post*. (July 25, 2002): A18.
- Schoch, Deborah. "Port Security Upgrade Welcomed, But Industry Asks Who Will Pay." *Los Angeles Times*. (February 6, 2003): B3.
- Schwartz, Nelson. "Learning from Israel." *Fortune*. January 21, 2002.
- Schweber, Bill. "FM Transmitter/Receiver Provides 433-MHz Link." *EDN* 47, no. 9 (April 18, 2002): 22.
- "Security's Growing Leftovers: Confiscated or Forgotten Objects Piling Up at Country's Airports." *Washington Post*. (February 4, 2003): E1.
- Seewald, Nancy. "CIDX Forms Cybersecurity Unit." *Chemical Week* 165, no. 2 (January 15, 2003): 20.
- Seffers, George I. "NIMA 'Inadequate' in Analyzing Spy Data." *Federal Computer Week* 15, no. 3 (February 5, 2001): 55.
- Seife, Charles. "Crucial Cipher Flawed, Cryptographers Claim." *Science* no. 5590 (2002): 2193.
- "September 11 Leaves Facility Pushed to Its Maximum." *Augusta Chronicle*. (Augusta, GA) (September 2, 2002): B5.
- Serino, Robert B. "Money Laundering, Terrorism, and Fraud." *ABA Bank Compliance*, (March/April 2002): 23–26.
- Settles, G.S., and W.J. McCann. "Potential for Portal Detection of Human Chemical and Biological Contamination." *SPIE Aerosense* no. 4378 (2001): paper 01.
- Shams, Heba. "Using Money Laundering Control to Fight Corruption: An Extraterritorial Instrument." *International Financial and Economic Law* no. 27 (2000).
- Shanker, Tom. "Largest Conventional Bomb Dropped in a Test in Florida." *New York Times*. March 12, 2003.
- Sharke, Paul. "The Start of a New Movement." *Mechanical Engineering* 124, no. 8 (August 2002): 47–49.
- Sipress, Alan. "Sudan Provides Administration Intelligence on Bin Laden." *Wall Street Journal*. (September 30, 2001): A14.
- Skoning, Gerald. "Be Careful Not to 'Tripp.'" *HR Magazine* 43, no. 6 (May 1998): 125–130.
- Skrzycki, Cindy. "Security in Mind, Customs Says Cargo Can Wait." *Washington Post*. (February 11, 2003): E1.
- Slusser, Robert M. "Recent Soviet Books on the History of the Soviet Security Police—Part II." *Slavic Review* 22 (Dec. 1973): 825–828.
- Smith, Bradley F. "An Idiosyncratic View of Where We Stand on the History of American Intelligence in the Early Post-1945 Era." *Intelligence and National Security* 3, no. 4 (Oct. 1988): 111–123.
- Smith, Ray A. "The Aesthetics of Security—Building Owners, Architects Seek to Make Properties Safer Without Look of a Fortress." *Wall Street Journal*. (February 19, 2003): B1.
- Solis, Suzanne Espinosa. "Software May Have Mapped N.Y. Hit." *San Francisco Chronicle*. (December 12, 2001): A11.
- Soltis, Dan. "Integrated Emergency Response Plans Will Save U.S. Industry Millions." *Water Engineering & Management* 144, no. 2 (February 1997): 17.
- Spencer, Debra D. "Vulnerability Assessment." *Corrections Today* 60, no. 4 (July 1998): 88–92.
- Squeo, Anne Marie. "Leading the News: U.S. Studies Using 'E-Bomb' in Iraq—Electromagnetic Weapon Can Permanently Damage Telecom, Power Systems." *Wall Street Journal*. (February 20, 2003): A3.
- Steinman, Adam H. "Streamline Your Facility's Emergency Response Plans." *Chemical Engineering* 106, no. 3 (March 1999): 102.
- Stephens, Joe, and Valerie Strauss. "Retaliation Alleged at CDC; Scientist Disclosed Diversion of Funds." *Washington Post*. (August 6, 1999): A19.
- Stern, Christopher. "Federal Radio Spectrum up for Bid." *Broadcasting & Cable* 124, no. 7 (February 14, 1994): 46.
- Stix, Gary. "Aging Airways." *Scientific American*. (May 1994).
- Stone, Richard. "Nuclear Trafficking: 'A Real and Dangerous Threat.'" *Science* no. 5522 (2001): 1632–1636.
- Strong, Ronald L. "The National Drug Intelligence Center: Assessing the Drug Threat." *The Police Chief* 68, no. 5 (May 2001): 55–60.

- Swanekamp, Robert. "Nuclear Renaissance Converges on Life Extension and Upgrades." *ENR* 247, no. 23 (December 3, 2001): PC54.
- Sykes, L.R. "Four Decades of Progress in Seismic Identification Help Verify the CTBT." *Eos, Transactions, American Geophysical Union*, vol. 83, no. 44 (October 29, 2002): 497, 500.
- Tagliabue, J. "France and Russia Ready To Use Veto Against Iraq War." *New York Times*. March 6, 2003.
- Taubes, Gary. "Quantum Mechanics: To Send Data, Physicists Resort to Quantum Voodoo." *Science* 274 (Oct. 25, 1996): 504–505.
- "Tech 101: Hollywood's Caller ID Hang-Up." *Los Angeles Times*. (May 24, 2001): T1.
- Terpstra, David E., et al. "The Nature of Litigation Surrounding Five Screening Devices." *Public Personnel Management* 29, no. 1 (spring 2000): 43–54.
- "Texas Politicians' Cases Prompt New Interest in Eavesdropping." *San Francisco Chronicle*. (December 18, 1995): A12.
- "Thabo's Watching: Spying in South Africa." *The Economist* 362, no. 8266 (March 30, 2002): 41.
- Thomas, Evan. "The Road to September 11." *Newsweek*. 138, no. 14 (October 1, 2001): 38–49.
- Thompson, Cheryl W. "Lawmaker Faults Nuclear Facility Security Policies." *Washington Post*. (March 25, 2002): A17.
- Thompson, Loren B. "The Lessons of 'Enduring Freedom.'" *Wall Street Journal*. (January 7, 2002): A24.
- Thompson, Neal. "Preparing for Disaster." *The Sun*. (Baltimore, MD) (March 13, 1998): 3B.
- Thompson, Phillip. "A Crystal Ball for Intelligence Needs." *Sea Power*, vol. 44, no. 3 (March 2001): 51–53.
- Thormann W., Y. Aebi, M. Lanz, and J. Caslavka. "Capillary Electrophoresis in Clinical Toxicology." *Forensic Sci Int.* 92 (1998): 157–83.
- Torregrosa-Penalva, German, et al. "Microwave Temperature Compensated Detector Design for Wide Dynamic Range Applications." *Microwave Journal* 44, no. 5 (May 2001): 336–346.
- "Training Centers Offer Assistance." *Crime Control Digest* 36, no. 18 (May 3, 2002): 11.
- Treaster, Joseph B. "Insurance for Terrorism Still a Rarity." *New York Times*. (March 8, 2003): C1.
- Treherne, Jan. "Robotic Roads—Pathways to the Future." *The Industrial Robot* 21, no. 5 (1994): 3.
- "TRIA Already Is a Success." *Business Insurance* 37, no. 8 (February 24, 2003): 8.
- "Tuition-Free, Counter-Drug Courses Offered." *National Guard* 54, no. 10 (October 2000): 10.
- Turco, R.P., A.B. Toon, T.P. Ackerman, et al. "Nuclear Winter: Global Consequences of Multiple Nuclear Explosions." *Science* no. 222 (1983): 1283–1297.
- U.S. Congress. Office of Technology Assessment. *Starpower: The U.S. and the International Quest for Fusion Energy*. Washington, D.C.: Office of Technology Assessment, 1987.
- U.S. Congress. Senate. Select Committee on Intelligence. *Economic Intelligence. Hearing, 103d Congress, 1st Session*. Washington, DC: GPO, 1994.
- "U.S. Homeland Security: Behind the Curve in Funding and Commitment." *Aviation Week & Space Technology* 158, no. 9 (March 3, 2003): 66.
- "Upgrades for P-3s to Begin in 1998." *Aviation Week & Space Technology* 146, no. 13 (March 31, 1997): 33.
- "USPS Builds to Sterilize Mail." *Engineering News-Record* no. 247 (November 26, 2001): 11.
- Vedantam, Shankar. "The Polygraph Test Meets Its Match." *Washington Post*. (November 12, 2001): A2.
- Verton, Dan. "National IT Protection Plan Update Delayed." *Computerworld* 35, no. 41 (October 8, 2001): 12.
- Verton, Dan. "NIPC Warns of Attacks, But No Impact Felt." *Computerworld* 36, no. 33 (August 12, 2002): 17.
- "Victory in the War on Terrorism Will Not Be Won on the Defensive." *New York Times*. (September 10, 2002): A19.
- "Virus Hits A.T.M.'s and Computers Across Globe." *New York Times*. January 28, 2003.
- Vise, David A. "Senate Panel Blasts FBI's Deployment." *Washington Post*. (July 21, 2000): A29.
- Vogel, Steve. "Cooler Name Prevails for 'Hot' New Marine Corps Club at Indian Head." *Washington Post*. (April 26, 2001): T15.
- Wald, Matthew L. "Guards at Nuclear Plants Say They Feel Swamped by a Deluge of Overtime." *New York Times*. October 20, 2002.
- Wald, Matthew L. "New Rule to Limit Boarding Passes from Gate." *New York Times*. (December 10, 2002): A24.
- Wald, Matthew L. "Some Busy Airports to Miss Deadline for Scanning Bags." *New York Times*. (November 19, 2002): A23.
- Waldron, Ronald J. "National Institute of Justice Helps Facilities Implement Telemedicine Program." *Corrections Today* 64, no. 2 (April 2002): 184.
- Wall, Robert. "Conflict Could Test Special Ops Improvements." *Aviation Week & Space Technology* 155, no. 14 (October 1, 2001): 30–31.
- Wall, Robert. "Focus on Iraq Shapes Electronic, Info Warfare." *Aviation Week & Space Technology* 157, no. 19 (November 4, 2002): 34–35.
- Wall, Robert. "Intelligence Support Seen Crucial to U.N." *Aviation Week & Space Technology* 157, no. 17 (October 21, 2002): 30.
- Wall, Robert. "New Arms Policies Seen Altering Warfare." *Aviation Week & Space Technology* 155, no. 10 (September 3, 2001): 100.
- Wall, Robert. "Review of NMD Fallout Underway." *Aviation Week & Space Technology* 152, no. 19 (May 8, 2000): 31–32.
- Wallace, T.C. "The May 1998 India and Pakistan Nuclear Tests." *Seismic Research Letters*, vol. 69 (1998): 386–393.
- Waller, Douglas. "The Secret Bomb Squad." *Time*. (March 18, 2002): 23.
- Wallgren, Christine. "EPA Team Does Its Work Behind the Scenes." *Boston Globe*. (August 1, 2002): 1.
- Walter, K. "A Two-Pronged Attack on Bioterrorism." *Science & Technology*, June (2002): 4–11.
- Wang, Wallace. "Hardening Your System." *Boardwatch* 15, no. 8 (June 2001): 44–46.

- "War Spurs Aerosol Research." *Geotimes* 37 (1992): 10–11.
- Warchol, Glen. "Beam Us Up, Scotty: 'Tricorder' May Fight Biological Threats." *Salt Lake Tribune*. (May 7, 2001): D1.
- Warden, John A. III. "The New American Security Force." *Airpower Journal* 13, no. 3 (fall 1999): 75–91.
- Warner, Tom. "U.S. Plans to Shun Ukraine President over Radar." *Financial Times*. (November 9, 2002): 10.
- Watts, John M., Jr. "Our Changing World." *Fire Technology* 38, no. 2 (April 2002): 99–100.
- Waugh, William L., Jr., and Richard T. Sykes. "Organizing the War on Terrorism." *Public Administration Review* 62, special issue (September 2002): 145–153.
- Weckerle, J.F. "Domestic Preparedness for Events Involving Weapons of Mass Destruction." *Journal of the American Medical Association* no. 283 (1997): 435–438.
- Weinberger, Caspar, and Peter Schweizer. "...But We've Defeated Terrorists Before." *USA Today*. (September 24, 2001): A15.
- Weiner, Tim. "Along Borders, Tension and Uncertainty Prevail." *New York Times*. (March 1, 2003): A11.
- Weiser, Carl. "'Secret' Government Site Not So Secret After All." *USA Today*. (June 26, 2002).
- Wertner, C., and J. Bilbro. "Coherent Laser Radar: Technology and Applications." *Proceedings of the SPIE*, vol. 1181 (1989).
- "What a Laser Can and Cannot Do." *San Jose Mercury News*, (February 1994): 22, 24.
- White, Ben. "Commerce Secretary Unveils New Security Policy." *Washington Post*. (February 11, 1998): A19.
- Williams, Dillwyn. "Cancer After Nuclear Fallout: Lessons From the Chernobyl Accident." *Nature Reviews*, vol. 2 (July, 2002): 543–549.
- Williams, Krissah. "U.S. Seeks to Build Secure Online Network." *Washington Post*. (October 11, 2001): A10.
- Williamson, Hugh. "Libya Blamed for 1986 Berlin Disco Bombing." *Financial Times*. (November 14, 2001): 12.
- Wilson, George C. "Drug-War Radar Picks up a Funding Blip." *Washington Post*. (April 14, 1987): A21.
- Wilson, Jim. "E-Bomb." *Popular Mechanics*. 178, no. 9 (September 2001): 50–53.
- Wolkowitz, Dave. "Facility Security—Playing It Safe." *Area Development Site and Facility Planning* 37, no. 9 (September 2002): 72.
- Wong, S.H. "Challenges of Toxicology for the Millennium." *Ther Drug Monit.* 22 (2000): 52–7102.
- Wong, Z., V. Wilson, A.J. Jeffereys, et al. "Cloning a Selected Fragment from a Human DNA 'Fingerprint': Isolation of an Extremely Polymorphic Minisatellite." *Nucleic Acids* no. 14 (1986): 4605–46
- Wright, Andrew J., et al. "War, Recession, and Growth." *ENR* 249, no. 2 (July 8, 2002): 34–36.
- Wright, Karen. "Go Ahead, Try to Lie." *Discover*. 22, no. 7 (July 2001): 21–22.
- Wyman, A.R. and R. White. "A Highly Polymorphic Locus in Human DNA." *PNAS* no. 77 (1980): 6754–6758.
- "Young Defends \$13 Billion CVN-21 Development Investment." *Defense Daily* 217, no. 32 (February 19, 2003): 1.
- Young, Emma. "Brain Scans Can Reveal Liars." *New Scientist* (November 12, 2001).
- Zelikow, Philip. "The Global Infectious Disease Threat and Its Implications for the United States." *Foreign Affairs* 79, no. 4 (July/August 2000): 154–155.
- ZoBell, C.E. "Bacteria as Geological Agents with Particular Reference to Petroleum." *Petroleum World* no. 10 (January 1943): 30–43.

## Internet Sites

- African Issues. U.S. Department of State. <<http://usinfo.state.gov/regional/af/>> (April 29, 2003).
- Air Force Office of Special Investigations. <<http://www.dtic.mil/afosi/>> (December 29, 2002).
- American Academy of Forensic Science. <<http://www.aafs.org.>> (February 7, 2003)
- American Polygraph Association. <<http://www.polygraph.org/>> (April 15, 2003).
- American Society for Microbiology. "Careers in the Microbiological Sciences." 2000. <<http://www.asmta.org/educ/edu21.htm>> (January 22, 2002).
- Arizona Department of Health Services: Epidemiology and Surveillance. "History of Biowarfare and Bioterrorism." <<http://www.hs.state.az.us/phs/edc/edrp/es/bthistor2.htm>>(March 12, 2003).
- Army Security Agency Online. <<http://www.asa.npoint.net>> (December 30, 2002).
- Australian Secret Intelligence Service. <<http://www.asis.gov.au/>> (April 1, 2003).
- Australian Security Intelligence Organization. <<http://www.asio.gov.au/>> (April 1, 2003).
- Bacteria Museum. "Special Feature: Bacterial Diseases in History." 2002. <<http://www.bacteriamuseum.org/niches/features/diseasehistory.htm>> (April 30, 2002).
- Bartlett, David. *A Concise Reference Guide to the Metric System*. <<http://www.bms.abdn.ac.uk/undergraduate/guidetounits.html>> (2002).
- Biosensor Technologies. <<http://www.darpa.mil/dso/thrust/biosci/biosensor/index.html>> (March 11, 2003).
- Brookhaven National Laboratory. <<http://www.bnl.gov/world/>> (April 2, 2003).
- Brookings Institution. <<http://www.brookings.edu>> (February 27, 2003).
- Bureau for International Narcotics and Law Enforcement Affairs. <<http://www.state.gov/g/inl/>> (March 19, 2003).
- Bureau of Alcohol, Tobacco, and Firearms. <<http://www.atf.treas.gov>> (December 30, 2002).
- Bureau of Citizenship and Immigration Services. INSPASS. March 1, 2003. <<http://www.immigration.gov/graphics/howdoi/inspassloc.htm>> (April 14, 2003).
- Bureau of Engraving and Printing. <<http://www.bep.treas.gov/>> (February 5, 2003).
- Bureau of Intelligence and Research. U.S. Department of State. <<http://www.state.gov/s/inr/>> (April 7, 2003).

- Careers in Intelligence. Association of Former Intelligence Officers. <<http://www.afio.com/sections/careers/>> (April 30, 2003).
- CDC. "Severe Acute Respiratory Syndrome (SARS)." April 3, 2003. <<http://www.cdc.gov/ncidod/sars/isolationquarantine.htm>> (April 27, 2003).
- CDI (Center for Defense Information), Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <<http://www.cdi.org/terrorism/terrorist.cfm>> (April 17, 2003).
- Center for Strategic and International Studies. <<http://www.csis.org/>> (February 27, 2003).
- Centers for Disease Control. "Anthrax." 2001. <[http://www.cdc.gov/ncidod/dbmd/diseaseinfo/anthrax\\_t.htm](http://www.cdc.gov/ncidod/dbmd/diseaseinfo/anthrax_t.htm)> (January 27, 2002).
- Centers for Disease Control. "Biological Diseases/Agents Listing." 2001. <<http://www.bt.cdc.gov/Agent/Agentlist.asp>> (January 23, 2002).
- Centers for Disease Control. "Ebola Hemorrhagic Fever." 2001. <<http://www.cdc.gov/ncidod/dvrd/spb/mnpages/dispages/ebola.htm>> (March 12, 2003).
- Centers for Disease Control. "Viral Hemorrhagic Fevers." 2000. <<http://www.cdc.gov/ncidod/dvrd/spb/mnpages/dispages/vhf.htm>> (March 12, 2003).
- Centers for Disease Control. "Yellow Fever: Disease and Vaccine." 2001. <<http://www.cdc.gov/ncidod/dvbid/yellowfever/index.htm>> (March 12, 2003).
- Centers for Disease Control and Prevention. "About CDC." November 2, 2002. <<http://www.cdc.gov/aboutcdc.htm>> (December 28, 2002).
- Centers for Disease Control and Prevention: "Facts About Sarin." <<http://www.bt.cdc.gov/agent/sarin/basics/facts.asp>> (March 25, 2003).
- Central Intelligence Agency. <<http://www.cia.gov/>> (April 24, 2003).
- Central Intelligence Agency. "Center for Studies of Intelligence." <<http://www.cia.gov/csi/>> (January 17, 2003).
- Central Intelligence Agency. Federation of American Scientists. <<http://www.fas.org/irp/cia/index.html>> (April 24, 2003).
- Central Intelligence Agency. "The Global Infectious Disease Threat and Its Implications for the United States." January 2000. <<http://www.cia.gov/cia/publications/nie/report/nie99-17d.html>> (November 22, 2002).
- Central Intelligence Agency. "Key Events in CIA's History." <<http://www.cia.gov/cia/publications/facttell/keyevent.htm>> (January 2, 2003).
- Central Intelligence Agency. *The Office of Strategic Services: America's First Intelligence Agency*. <<http://www.cia.gov/cia/publications/oss/>> (March 1, 2003)
- Central Intelligence Agency. World Factbook, 2002. <<http://www.cia.gov/cia/publications/factbook/>> (April 16, 2003).
- Chemical and Biological Information Analysis Center. <<http://www.cbiac.apgea.army.mil/>> (January 17, 2003).
- "The CERN Archive." <<http://library.cern.ch/archives/index.html>> (March 11, 2003).
- CIA Careers. Central Intelligence Agency. <<http://www.cia.gov/employment/>> (April 30, 2003).
- CIA Museum. Central Intelligence Agency. <<http://www.cia.gov/cia/information/artifacts/>> (March 29, 2003).
- Coast Guard National Response Center. <<http://www.nrc.uscg.mil/index.htm>> (January 22, 2003).
- Communications Electronics Security Group. <<http://www.cesg.gov.uk/>> (April 12, 2003).
- "The Comprehensive Nuclear Test-Ban Treaty." United States Department of State. <<http://www.state.gov/www/global/arms/treaties/ctb.html>> (March 10, 2003).
- Computer Security Division. National Institute of Standards and Technology. <<http://csrc.nist.gov>> (January 28, 2003).
- Coordinator for Counterterrorism. United States Department of State. <<http://www.state.gov/s/ct/>> (February 22, 2003).
- Council on Foreign Relations. "Loose Nukes." 2003. <[http://www.terrorismanswers.com/weapons/loosenukes\\_print.html](http://www.terrorismanswers.com/weapons/loosenukes_print.html)> (February 28, 2003).
- Counterfeit Detection: A Guide to Spotting Counterfeit Currency. <<http://www.indigoimage.com/>> (February 5, 2003).
- Counterterrorism and Incident Response. Lawrence Livermore National Laboratory. <<http://www.llnl.gov/nai/rdiv/rdiv.html>> (April 2, 2003).
- Counterterrorism Policy. University of Pittsburgh School of Law. <<http://jurist.law.pitt.edu/terrorism/terrorism2.htm>> (May 1, 2003).
- Court Technology Laboratory. "Biometrics and the Courts. Individual biometrics." <<http://ctl.ncsc.dni.us/>>(December 14, 2002).
- Critical Infrastructure Assurance Office. <<http://www.ciao.gov>> (January 28, 2003).
- Declassification and Freedom of Information Act (FOIA). Defense Prisoner of War/Missing Personnel Office. <<http://www.dtic.mil/dpmpo/foia/>> (January 21, 2003).
- Declassified Intelligence Satellite Photographs. <<http://mac.usgs.gov/isb/pubs/factsheets/fs09096.html>> (February 13, 2003).
- Defense Advanced Research Projects Agency. <<http://www.darpa.mil/>> (April 14, 2003).
- Defense Advanced Research Projects Agency, Defense Science Office. Continuous Assisted Performance (CAP). <<http://www.darpa.mil/dso/thrust/biosci/cap.htm>> (April 14, 2003).
- Defense Department Space Policy. Federation of American Scientists. <[http://www.fas.org/spp/military/docops/defense/d5105\\_19.htm](http://www.fas.org/spp/military/docops/defense/d5105_19.htm)> (February 22, 2003).
- Defense Information Systems Agency. <<http://www.disa.mil/>> (February 22, 2003).
- Defense Intelligence Agency. <<http://www.dia.mil/>> (April 14, 2003).
- Defense Intelligence Agency. Federation of American Scientists. <<http://www.fas.org/irp/dia/>> (April 14, 2003).
- Defense Language Institute Foreign Language Center. <<http://pom-www.army.mil/>> (April 4, 2003).
- Defense Nuclear Facilities Safety Board. <<http://www.dnfsb.gov>> (February 22, 2003).
- Defense Security Service. <<http://www.dss.mil/>> (February 22, 2003).
- Department of Energy. <<http://www.energy.gov>> (March 7, 2003).

- Department of Energy Office of Security. <<http://www.so.doe.gov>> (March 7, 2003).
- Department of Homeland Security. April 2, 2003. <<http://www.dhs.gov/dhspublic/index.jsp>> (April 11, 2003).
- Department of Homeland Security, Bureau of Citizenship and Immigration Services. Law Enforcement: The National Border Patrol Strategy. <<http://www.immigration.gov/graphics/publicaffairs/statements/igstate.htm>> (April 12, 2003).
- Department of Homeland Security Reorganization. C-SPAN. <<http://www.c-span.org/homelandsecurity/chart.asp>> (April 11, 2003).
- Department of State. U.S. Intelligence Community. <[http://www.intelligence.gov/1-members\\_state.shtml](http://www.intelligence.gov/1-members_state.shtml)> (April 7, 2003).
- Digital Globe. <<http://www.digitalglobe.com/>>(April 12, 2003).
- Directorate of Science and Technology. Central Intelligence Agency. <<http://www.cia.gov/cia/dst/home.html>> (April 24, 2003).
- Drug Enforcement Administration. <<http://www.dea.gov>> (March 13, 2003).
- Dual Use Science and Technology Program. <<http://www.dtic.mil/dust/>> (April 14, 2003).
- Earthshots: Satellite Images of Environmental Change (U.S. Geological Survey). <<http://edcwww.cr.usgs.gov/earthshots/slow/tableofcontents>> (February 26, 2003).
- "Electromagnetic Spectrum Use in Joint Military Operations." Chairman of the Joint Chiefs of Staff Instruction. May 1, 2000. <[http://www.dtic.mil/doctrine/jel/cjcsd/cjcsi/3320\\_01.pdf](http://www.dtic.mil/doctrine/jel/cjcsd/cjcsi/3320_01.pdf)> (January 30, 2003).
- Emergency Response Program, National Response Team. Environmental Protection Agency. <<http://www.epa.gov/superfund/programs/er/nrs/nrsnt.htm>> (March 30, 2003).
- Environmental Measurements Laboratory. National Security. <<http://www.eml.doe.gov/>> (March 16, 2003).
- Environmental Protection Agency, Office of Water 2002. <<http://www.epa.gov/owow/estuaries/about1.htm>> (May, 11, 2002).
- EPA's Radiation Protection Program: Emergency Response. Environmental Protection Agency. <<http://www.epa.gov/radiation/ert/history.htm>> (March 4, 2003).
- Evaluation Report on Measurement and Signature Intelligence. <[http://www.fas.org/irp/program/masint\\_evaluation\\_rep.htm](http://www.fas.org/irp/program/masint_evaluation_rep.htm)> (January 17, 2003).
- Executive Orders. National Archives and Records Administration. <[http://www.archives.gov/federal\\_register/executive\\_orders/executive\\_orders.html](http://www.archives.gov/federal_register/executive_orders/executive_orders.html)>(January 22, 2003).
- FBI Laboratory Explosives Unit. <<http://www.fbi.gov/hq/lab/org/eu.htm>> (January 16, 2003).
- Federal Bureau of Investigation. <<http://www.fbi.gov>> (May 4, 2003).
- Federal Emergency Management Agency. <<http://www.fema.gov>> (March 26, 2003).
- Federal Energy Regulatory Commission. <<http://www.ferc.fed.us/>> (February 23, 2003).
- Federal Law Enforcement Training Center. <<http://www.fletc.gov>> (March 19, 2003).
- Federal Radiological Emergency Response Plan. Florida Department of Community Affairs. <<http://www.dca.state.fl.us/bpr/EMTOOLS/Nuclear/frerp.htm>> (March 4, 2003).
- Federal Reserve Board. <<http://www.federalreserve.gov/>> (February 5, 2003).
- Federation of American Scientists. "Central Intelligence Agency." September 23, 1996. <<http://www.fas.org/irp/cia/ciahist.htm>> (January 2, 2003).
- Federation of American Scientists, FAS Intelligence Resource Program. "Soviet/Russian Intelligence Agencies." <<http://www.fas.org/irp/world/russia/>> (April 18, 2003).
- Foreign Emergency Support Team. U.S. Department of State. <<http://www.state.gov/s/ct/rls/fs/2002/13045.htm>> (February 23, 2003).
- Foreign Service Institute. <<http://www.state.gov/m/fsi/>> (April 4, 2003).
- Forensic Science Center , University of California Lawrence Livermore National Laboratory. <<http://www.llnl.gov/IPandC/op96/10/10h-for.html>> (7 February 2003)
- Freedom of Information Act (FOIA). U.S. Department of Justice. <<http://www.usdoj.gov/04foia/>> (March 16, 2003).
- GAO Report: Patriot Missile Defense. Federation of American Scientists. <<http://www.fas.org/spp/starwars/gao/im92026.htm>> (April 7, 2003).
- General Accounting Office. <<http://www.gao.gov/>> (February 23, 2003).
- General Services Administration. <<http://www.gsa.gov/>> (February 23, 2003).
- Global Analytic Information Technology Services. "Retinal Scanning." <[http://www.gaits.com/biometrics\\_retinal.asp](http://www.gaits.com/biometrics_retinal.asp)> (December 14, 2002).
- Government Communications Headquarters. <<http://www.gchq.gov.uk/>> (April 12, 2003).
- "Guide to the Technologies of Concealed Weapon and Contraband Imaging and Detection (NIJ Guide 602-00)." Institute of Justice, U.S. Department of Justice. February, 2001. <<http://www.ojp.usdoj.gov/nij/pubs-sum/184432.htm>> (April 23, 2003).
- Haze Gray and Underway World Aircraft Carrier Lists. <<http://www.hazegray.org/navhist/carriers/>> (April 13, 2003).
- Heritage Foundation. <<http://www.heritage.org>> (February 27, 2003).
- History of the National Security Council. American Federation of Scientists. <<http://www.fas.org/irp/offdocs/NSChistory.htm>> (March 24, 2003).
- Hoover Institution. <<http://www-hoover.stanford.edu>> (February 27, 2003).
- Human Genome Project. "From the Genome to the Proteome." <[http://www.ornl.gov/TechResources/Human\\_Genome/project/info.html](http://www.ornl.gov/TechResources/Human_Genome/project/info.html)> (March 14, 2003).
- ID Theft Resource Center. "ID Theft." October 28, 2002. <<http://www.idtheftcenter.org/>> (December 1, 2002).
- Imagery Intelligence. Federation of American Scientists. <<http://www.fas.org/irp/imint/>> (April 3, 2003).
- ImageSat International. <<http://www.imagesatintl.com/>>(12 April 2003).
- Information Warfare and Information Security on the Web. Federation of American Scientists. <<http://www.fas.org/irp/wwwinfo.html>> (April 14, 2003).

- The Information Warfare Site. <<http://www.iwar.org.uk/>> (April 14, 2003).
- Institute for Genomic Research. "About TIGR." 2002. <<http://www.tigr.org/about/>> (May 3, 2002).
- Institute for the Advanced Study of Information Warfare. <<http://www.psycom.net/iwar.1.html>> (April 14, 2003).
- Intelligence Agency Profiles. Federation of American Scientists. <<http://www.fas.org/irp/agency/>> (April 14, 2003).
- Internal Revenue Service. <<http://www.irs.gov/>> (April 4, 2003).
- International Atomic Energy Agency (IAEA). 2003. <<http://www.iaea.org/worldatom/>> (April 2, 2003).
- International Committee of the Red Cross. "Depleted Uranium Munitions." June 6, 2001. <<http://www.icrc.org/Web/eng/siteeng0.nsf/htmlall/57JR5D?OpenDocument>> (March 6, 2003).
- International Spy Museum. <<http://www.spymuseum.org/>> (January 31, 2003).
- The Internet Dermatology Society. "Biological Warfare and its Cutaneous Manifestations." <<http://telemedicine.org/BioWar/biologic.htm>> (May 10, 2002).
- Jane's. <<http://www.janes.com>> (February 27, 2003).
- Jasinski, Michael. "Nonproliferation Assistance to Russia and the New Independent States." Center for Nonproliferation Studies for the Nuclear Threat Initiative. August 2002. <[http://www.nti.org/e\\_research/e3\\_4b.html](http://www.nti.org/e_research/e3_4b.html)> (February 28, 2003).
- Lawrence Livermore National Laboratories. "Chemical and Biological Detection Technologies." <<http://www.llnl.gov/nai/rdiv/chbio.html>> (January 15, 2003).
- "The Limited Nuclear Test-Ban Treaty." United States Department of State. <<http://www.state.gov/t/ac/trt/4797.htm>> (March 10, 2003).
- Los Alamos National Laboratory. <<http://www.lanl.gov/worldview/>> (March 23, 2003).
- MI5: The Security Service. <<http://www.mi5.gov.uk/>> (April 11, 2003).
- National Atmospheric Release Advisory Center. <<http://narac.llnl.gov/>> (January 14, 2003).
- National Center for Forensic Science, University of Central Florida. <<http://ncfs.ucf.edu/navbar.html>> (February 7, 2003).
- National Communication System. <<http://www.ncs.gov>> (January 29, 2003).
- National Domestic Preparedness Office. Federation of American Scientists. <<http://www.fas.org/irp/agency/doj/fbi/ndpo/>> (March 28, 2003).
- National Drug Intelligence Center. <<http://www.usdoj.gov/ndic/>> (February 23, 2003).
- National Foreign Language Center. University of Maryland. <<http://www.nflc.org/>> (April 4, 2003).
- National Human Genome Research Institute. "Ethical, Legal and Social Implications of Human Genetic Research." (October 2000). <<http://www.nhgri.nih.gov/ELSI/>> (June 15, 2002).
- National Imagery and Mapping Agency. "Shuttle Radar Topography Mission Navigation Page." October 11, 2002. <<http://www.nima.mil/srtm/navigation.html>> (December 9, 2002).
- National Infrastructure Protection Center. <<http://www.nipc.gov>> (March 4, 2003).
- National Institute of Justice. <<http://www.ojp.usdoj.gov/nij/>> (March 28, 2003).
- National Institute of Mental Health <<http://www.nimh.nih.gov/>> (December 7, 2002).
- National Institute of Standards and Technology. <<http://www.nist.gov/>> (January 28, 2003).
- National Institutes of Health. <<http://www.nih.gov>> (January 1, 2003).
- National Intelligence Council. <<http://www.cia.gov/nic/>> (March 17, 2003).
- National Interagency Civil-Military Institute. <<http://www.nici.org/>> (March 30, 2003).
- National Maritime Intelligence Center/Office of Naval Intelligence. <<http://www.nmic.navy.mil/nmicpic.htm>> (January 17, 2003).
- National Nuclear Security Administration. <<http://www.nnsa.doe.gov>> (March 7, 2003).
- National Oceanic & Atmospheric Administration (NOAA). <<http://www.noaa.gov>> (May 10, 2003).
- National Reconnaissance Office. <<http://www.nro.gov/>> (April 1, 2003).
- National Science Foundation. <<http://www.nsf.gov>> (January 15, 2003).
- National Security Agency. <<http://www.nsa.gov/>> (March 24, 2003).
- National Security Agency. Federation of American Scientists. <<http://www.fas.org/irp/nsa/index.html>> (March 24, 2003).
- National Security Council. <<http://www.whitehouse.gov/nsc/>> (March 24, 2003).
- National Security Strategy of the United States of America. <<http://www.whitehouse.gov/nsc/nss.html>> (March 18, 2003).
- National Security Telecommunications Advisory Committee. <<http://www.ncs.gov/NSTAC/nstac.htm>> (February 2, 2003).
- National Technology Transfer Center. <<http://www.nttc.edu>> (March 18, 2003).
- National Telecommunications and Information Administration. <<http://www.ntia.doc.gov/>> (March 28, 2003).
- National Weather Service. <<http://www.nws.noaa.gov>> (April 30, 2003).
- NATO. "North Atlantic Treaty Organisation." January 31, 2003. <<http://www.nato.int/>> (February 1, 2003).
- Naval Criminal Investigative Service. <<http://www.ncis.navy.mil>> (January 18, 2003).
- Naval Special Warfare. <<http://www.sealchallenge.navy.mil>> (April 1, 2003).
- NSA Career Center. National Security Agency. <<http://www.nsa.gov/programs/employ/homepage.html>> (April 30, 2003).
- "Nuclear Security—Before and After September 11." U.S. Nuclear Regulatory Commission. September 23, 2002. <<http://www.nrc.gov/what-we-do/safeguards/response-911.html>> (December 11, 2002).
- Office of Domestic Preparedness. U.S. Department of Justice. <<http://www.ojp.usdoj.gov/odp/>> (March 28, 2003).
- Office of Information Security. General Service Administration Federal Technology Service. <<http://www.fts.gsa.gov/infosec/>> (March 4, 2003).



- Office of Intelligence Policy and Review. Department of Justice. <<http://www.usdoj.gov/oipr/>> (March 15, 2003).
- Office of Intelligence Support. Federation of American Scientists. <<http://www.fa.org/irp/agency/ustreas/tdois.htm>> (March 17, 2003).
- Office of the National Counterintelligence Executive. <<http://www.ncix.gov>> (March 17, 2003).
- Office of the Public Health Service Historian. <<http://lhncbc.nlm.nih.gov/apdb/phsHistory.>> (October 19, 2000).
- Office of the Surgeon General. <<http://www.surgeongeneral.gov/>> (April 2, 2003).
- Official Intelligence Documents. American Federation of Scientists. <<http://fas.org/irp/offdocs/>> (March 24, 2003).
- Online Career Center. Intelligence Careers. <[http://www.intelligencecareers.com/\\_homeroom/index.cfm](http://www.intelligencecareers.com/_homeroom/index.cfm)> (April 30, 2003).
- Pharmaceutical Researchers and Manufacturers of America "Genomics: A Global Resource" <<http://genomics.phrma.org/>> (April 3, 2003).
- Physicians and Scientists for Responsible Application of Science and Technology. "How Are Genes Engineered?" 2001. <<http://www.psrast.org/whisge.htm>> (June 15, 2002).
- Plum Island Animal Disease Center. <<http://www.ars.usda.gov/plum/index.html>> (March 23, 2003).
- Port Security Units. U.S. Coast Guard. <<http://www.uscg.mil/hq/g-cp/comrel/factfile/Factcards/PSUs.html>> (March 29, 2003).
- Poxvirus Bioinformatics Resource Center <<http://www.poxvirus.org/>> (April 1, 2003).
- Pravda. <<http://english.pravda.ru/>> (April 30, 2003).
- Press Briefing by Richard Clarke, National Coordinator for Security, Infrastructure Protection, and Counterterrorism. Federation of American Scientists. <<http://www.fas.org/irp/news/1998/05/980522-wh3.htm>> (March 26, 2003).
- RAND. <<http://www.rand.org>> (February 27, 2003).
- RCRA, Superfund, and EPCRA Call Center. <<http://www.epa.gov/epaoswer/hotline/>> (January 29, 2003).
- Remote Sensing Data and Information. <<http://rsd.gsfc.nasa.gov/rsd/RemoteSensing.html>> (February 26, 2003).
- Render Safe, Defusing a Nuclear Emergency. Los Alamos National Laboratory. Fall 2002. <[http://www.lanl.gov/quarterly/q\\_fall02/render\\_safe.shtml](http://www.lanl.gov/quarterly/q_fall02/render_safe.shtml)> (March 26, 2003).
- Resources for Law Enforcement. Anti-Defamation League. <[http://www.adl.org/learn/additional\\_resources/default.asp](http://www.adl.org/learn/additional_resources/default.asp)> (April 29, 2003).
- Rhode Island Department of Health: Bioterrorism Preparedness Program. "History of Biological Warfare and Current Threat." <<http://www.healthri.org/environment/biot/history.htm>> (March 12, 2003).
- Richelson, Jeffrey T. Science, Technology and the CIA. National Security Archive, George Washington University. <<http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB54/index2.html>> (April 24, 2003).
- Royal College of Pathologists. "Medical Microbiology." 2002. <<http://www.rcpath.org/recruitment/microbiology.htm>> (January 22, 2002).
- Russian Informational Centre. Ministry for Press, Television, Radio Broadcasting and Mass Communications of the Russian Federation. <[http://www.infocentre.ru/eng\\_user/](http://www.infocentre.ru/eng_user/)> (April 30, 2003).
- Satellite Remote Sensing. University of Waterloo Faculty of Environmental Sciences. <<http://www.fes.uwaterloo.ca/crs/geog165/srs.htm>> (February 26, 2003).
- Schroeder, Norbert. "Radio Frequency Spectrum Allocations in the United States." National Telecommunications and Information Administration. July 1, 2000. <[http://www.ntia.doc.gov/osmhome/chart\\_00.htm](http://www.ntia.doc.gov/osmhome/chart_00.htm)> (January 30, 2003).
- Scripps Center for Mass Spectrometry. <<http://masspec.scripps.edu/information/intro/index.html>> (January 5, 2003).
- Security Policy Board Documents. Federation of American Scientists. <<http://www.fas.org/spp/spb/>> (April 2, 2003).
- September 11 Archive. <<http://september11.archive.org/>> (April 22, 2003).
- Short, Nicholas M., Sr. "The Remote Sensing Tutorial." NASA. October 22, 2002. <<http://rst.gsfc.nasa.gov/>> (November 14, 2002).
- Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001, Annual Report: On the Record Briefing." May 21, 2002. <<http://www.state.gov/s/ct/rls/rm/10367.htm>> (April 17, 2003).
- Terrorism Act 2000. Her Majesty's Stationery Office. <<http://www.hmso.gov.uk/acts/acts2000/20000011.htm>> (April 7, 2003).
- Terrorism Risk Insurance Program. U.S. Department of the Treasury. <<http://www.ustreas.gov/offices/domestic-finance/financial-institution/terrorism-insurance/>> (March 28, 2003).
- Terrorism/Counter-Terrorism Web Links. United States Institute of Peace. <<http://www.usip.org/library/topics/terrorism.html>> (May 1, 2003).
- The American Civil Defense Association. <<http://www.tacda.org/>> (April 11, 2003).
- The Center for Counterintelligence and Security Studies. <<http://www.cicentre.com>> (April 2003).
- Transportation Safety Administration. <<http://129.33.119.130/public/index.jsp>> (March 12, 2003).
- "Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Limitation of Anti-Ballistic Missile Systems, 944 U.N.T.S. 13." Nuclear Age Peace Foundation. 2002. <<http://www.nuclearfiles.org/docs/1972/720526-abm.html>> (December 9, 2002).
- U.S. Agency for International Development. <<http://www.usaid.gov/>> (April 25, 2003).
- U.S. Air Combat Command. <<http://www2.acc.af.mil/>> (April 13, 2003).
- U.S. Air Intelligence Agency. <<http://aia.lackland.af.mil/>> (April 13, 2003).
- U.S. Department of Defense. <<http://www.defenselink.mil/>> (April 28, 2003).
- U.S. Department of Homeland Security. <<http://www.dhs.gov/dhspublic/>> (April 10, 2003).
- U.S. Department of Justice. <<http://www.usdoj.gov/>> (April 14, 2003).
- U.S. Department of State. <<http://www.state.gov/>> (April 25, 2003).

- U.S. Department of Transportation. <<http://www.dot.gov/>> (April 3, 2003).
- U.S. Intelligence and Security Agencies. Federation of American Scientists. <<http://www.fas.org/irp/official.html>> (April 29, 2003).
- U.S. Intelligence Community. <<http://www.intelligence.gov/>> (April 14, 2003).
- U.S. Navy—The Aircraft Carriers. U.S. Navy Office of Information. <<http://www.chinfo.navy.mil/navpalib/ships/carriers/>> (April 13, 2003).
- U.S. Nuclear Regulatory Commission. <<http://www.nrc.gov/>> (April 15, 2003).
- United Kingdom Atomic Energy Authority. "Focus on Fusion" <<http://www.fusion.org.uk/focus/index.htm>> (March 29, 2003).
- United Kingdom Government. The Public Record Office. <<http://www.pro.gov.uk.htm>> (October 17, 2002).>
- United Kingdom Government. "UK government online." <<http://www.ukonline.gov.uk/Home/HOHome/1,1031,~801b22~fs~en,00.html>> (October 19, 2002)
- United Kingdom Government, Ministry of Defence. "Defence Issues; Science and Technology." September 3, 2002. <<http://www.mod.uk/issues/science.htm>> (October 17, 2002).
- United Kingdom Intelligence Agencies. Federation of American Scientists. <<http://www.fas.org/irp/world/uk/index.html>> (April 11, 2003).
- United Nations. <<http://www.un.org>> (April 1, 2003).
- United Nations. Security Council Resolution 1441. November 7, 2002. <<http://www.un.int/usa/sres-iraq.htm>> (March 23, 2003).
- United States Air Force Special Operations Command. <<http://www.afsoc.af.mil/>> (April 2, 2003).
- United States Air Force Wargaming Institute. <<http://www.cadre.maxwell.af.mil/wargame/main.htm>> (March 14, 2003).
- United States Army <<http://mrmc-www.army.mil/>> ( April 10, 2003).
- United States Army Corps of Engineers Topographic Engineering Center. "TEC Web Site." 2002. <<http://www.tec.army.mil/>> (February 11, 2003).
- United States Army Intelligence and Security Command. <<http://www.inscom.army.mil/>> (February 2, 2003).
- United States Army Medical Research Institute of Chemical Defense. <<http://chemdef.apgea.army.mil/>> (April 10, 2003).
- United States Army Soldier and Biological Chemical Command (SBCCOM). <<http://www.sbccom.army.mil/>> (January 27, 2003).
- United States Army Special Operations Command. <[http://www.bragg.army.mil/18abn/usa\\_special\\_operations\\_command.htm](http://www.bragg.army.mil/18abn/usa_special_operations_command.htm)> (April 2, 2003).
- United States Chemical Safety and Hazard Investigation Board. <<http://www.chemsafety.gov/about>> (January 19, 2003).
- United States Commission on Civil Rights. <<http://www.usccr.gov/>> (January 29, 2003).
- United States Congress 107th Congress 2nd Session. "Technology assessment in the war on terrorism and homeland security: the role of OTA" Committee Print. April 2002. <[http://www.fas.org/irp/congress/2002\\_hr/ota.html](http://www.fas.org/irp/congress/2002_hr/ota.html)> (December 15, 2002).
- United States Department of Agriculture. "The AQI Program at Airports." <<http://www.aphis.usda.gov/oa/pubs/detdog1.html>> (February 20, 2003).
- United States Department of Energy. *Atomic Century*. <[http://www.dpi.anl.gov/dpi2/hist\\_docs/treaties/start2.htm](http://www.dpi.anl.gov/dpi2/hist_docs/treaties/start2.htm)> (December 20, 2002).
- United States Department of Energy, Department of Fossil Reserves. <[http://www.fe.doe.gov/program\\_reserves.html](http://www.fe.doe.gov/program_reserves.html)> (March 2, 2003).
- United States Department of Energy, Office of Fusion Energy Sciences. "Welcome to the U.S. Fusion Energy Sciences Program." <<http://www.fofe.er.doe.gov/>> (March 30, 2003).
- United States Department of Energy, Office of Science. National Laboratories and User Facilities. <[http://www.sc.doe.gov/Sub/Organization/Map/national\\_labs\\_and\\_userfacilities.htm](http://www.sc.doe.gov/Sub/Organization/Map/national_labs_and_userfacilities.htm)> (March 23, 2003).
- United States Department of Homeland Security. Bureau of Citizenship and Immigration Services, PORTPASS. March 11, 2003. <<http://www.immigration.gov/graphics/howdoi/portpass.htm>> (April 9, 2003).
- United States Department of Homeland Security. Immigration Information, INSPASS. March 4, 2003. <<http://www.immigration.gov/graphics/shared/howdoi/inspass.htm>> (April 9, 2003).
- United States Department of Homeland Security. Research & Technology. <<http://www.dhs.gov/dhspublic/display?theme=27&content=374>> (March 23, 2003).
- United States Department of Justice. "National Drug Threat Assessment 2002." December 2001 <<http://www.usdoj.gov/ndic/pubs/716/>> (March 11, 2003).
- United States Department of State. Annual reports. <[http://www.state.gov/www/global/terrorism/annual\\_reports.html](http://www.state.gov/www/global/terrorism/annual_reports.html)> (April 16, 2003).
- United States Department of State. "Parties and Signatories of the Biological Weapons Convention" December 11, 2002. <<http://www.state.gov/t/ac/bw/fs/2002/8026.htm>> (February 25, 2003).
- United States Department of State Bureau of Arms Control <<http://www.state.gov/t/ac/>> (December 30, 2002).
- United States Department of the Treasury. <<http://www.ustreas.gov/>> (March 17, 2003).
- United States Department of the Treasury. U.S. Customs Service. <<http://www.customs.ustreas.gov/>>
- United States Department of Transportation. "United States Coast Guard." January 27, 2003. <<http://www.uscg.mil/USCG.shtm.asp>> (January 27, 2003).
- United States Environmental Protection Agency. "EPA's Role and Authority in Counter Terrorism" Chemical Emergency Preparedness and Prevention. <<http://yosemite.epa.gov/oswer/ceppoweb.nsf/content/ct-epro.htm#epa>> (February 15, 2003).
- United States Federal Bureau of Investigation. <<http://www.fbi.gov/libref/historic/famcases/hanssen/hanssen.htm#anchor26782>> (April 2003)
- United States Geological Survey. <<http://www.usgs.gov/>> (February 13, 2003).
- United States National Archives & Records Administration. <<http://www.archives.gov/>>
- United States National Oceanic & Atmospheric Administration. <<http://www.noaa.gov.>> (January 15, 2003)
- United States National Response Team. <<http://www.nrt.org/>> (March 30, 2003).

- United States National Security Agency. <<http://www.nsa.gov>>(January 3, 2003).
- United States National Transportation Safety Board. <<http://www.ntsb.gov>> (April 30, 2003).
- United States Secret Service. <<http://www.ustreas.gov/ussf/>> (February 5, 2003).
- United States Senate Select Committee on Intelligence. <<http://intelligence.senate.gov/>> (April 2, 2003).
- United States Strategic Command. <<http://www.stratcom.af.mil/>> (March 28, 2003).
- University of California at Los Angeles. "Anthrax as a Weapon." College of Letters and Science. February 2002. <<http://www.college.ucla.edu/webproject/micro12/m12webnotes/anthraxweapon.html>> (December 29, 2002).
- University of California. Southern Regional Library Facility. The history of microfilm: 1839 to present. December 3, 2002. <<http://www.srlf.ucla.edu/exhibit/text/BriefHistory.htm>>(March 10, 2003).
- "Using and Wearing Radiation Dosimeters." Princeton University: Environmental Health and Safety. <<http://www.princeton.edu/~ehs/UsingandWearingDosimetry.html>> (April 17, 2003).
- Vietnam War Declassification Project. Gerald R. Ford Library and Museum. <<http://www.ford.utexas.edu/library/exhibits/vietnam/>> (February 5, 2003).
- Voice of America. "About VOA." February 1, 2003. <<http://www.voanews.com/index.cfm>> (February 1, 2003)
- Whistleblower Disclosures. U.S. Office of Special Counsel. <<http://www.osc.gov/wbdisc.htm>> (April 2, 2003).
- White House. "History of the National Security Council, 1947–1997." <<http://www.whitehouse.gov/nsc/history.html>> (April 25, 2003).
- White House. "National Security." <<http://www.whitehouse.gov/response/index.html>> (April 27, 2003).
- White House. "President's Foreign Intelligence Advisory Board." <<http://www.whitehouse.gov/pfiab/>> (March 29, 2003).
- White House, News & Policies. President Details Project BioShield. February 3, 2003. <<http://www.whitehouse.gov/news/releases/2003/02/20030203.html>> (April 3, 2003).
- White House Office of National Drug Control Policy. <<http://www.whitehousedrugpolicy.gov/>> (February 22, 2003).
- Wilkins, Gus. "The DA-Notice Website—The Official Site of the Defence, Press, and Broadcasting Advisory Committee." <<http://www.dnotice.org.uk/index.htm>> (December 1, 2002).
- Wilson, Elizabeth. *Introduction to AMMOS Telemetry Processing*. Jet Propulsion Laboratory, NASA. October 18, 2001. <<http://tel.jpl.nasa.gov/~betsy/mm/intro.htm>> (November 14, 2002).
- Wired News. "DNA Tagging." Stewart Taggart. <<http://www.wired.com/news/print/0,1294,34774,00.html>> (January 15, 2003).
- Woolf, Amy F. "Nuclear Weapons in the Former Soviet Union: Location, Command, and Control." Congressional Research Service Report 91144. <<http://www.fas.org/spp/starwars/crs/91-144.htm>> (February 28, 2003).
- World Health Organization. Communicable Disease Surveillance & Response (CSR). April 24, 2003 <<http://www.who.int/csr/sars/en/>> (April 27, 2003)
- World Health Organization. WHO Fact Sheets, May 2003. <<http://www.who.int/health-topics/zoonoses.htm>> (May 12, 2003)

# Index

Page references include both a volume number and a page number (for example, 1:286 refers to volume 1, page 286). Boldface page references signify the location of main articles. *Italic page references indicate illustrations.*

## I A I

- Abbe, Ernst, 2:270
- ABMT. *See* Advanced biomedical technologies program (ABMT)
- ABM Treaty. *See* Anti-Ballistic Missile Treaty (1972)
- Abrams, Elliott, 2:156
- Abu Nidal Organization (ANO), **1:1**
- Abu Sayyf Group (ASG), **1:1–2**
- Abwehr, **1:2–3**, 2:64
- Acambis, Inc., 3:87
- ACC. *See* Air Combat Command (ACC)
- Acheson, Dean, 1:325
- Acoustic bullets. *See* Audio Amplifiers
- Acoustics and acoustic devices, 1:69–70
- Acoustic stealth. *See* Stealth technology
- Adams, John Quincy, 1:28
- ADF. *See* Allied Democratic Forces (ADF)
- ADFGX Cipher, **1:3–4**, 1:205, 1:4
- ADIO. *See* Australian Defense Intelligence Organization (ADIO)
- Adleman, Leonard, 1:286
- Advanced biomedical technologies program (ABMT), 1:119
- Advanced Encryption Standard, 1:227, 1:228, 1:291, 1:396
- Advance Passenger Information System (APIS), **1:44–45**, 3:72
- Aerial photography and reconnaissance, 1:73–76, 2:59  
balloon development for, 1:92
- Aeronautical and aerospace research (NASA), 2:298
- AES. *See* Atomic emission spectroscopy (AES)
- AFGE. *See* American Federation of Federal Employees (AFGE)
- Afghanistan  
Al-Qaeda base in, 1:27, 1:149, 3:68  
Communists in, 1:196  
Operation Enduring Freedom, 1:397–398, 2:274  
Soviet invasion of, 1:240
- Aflatoxin, **1:5**, 3:166
- AFOSI. *See* Air Force Office of Special Investigations (AFOSI)
- Africa  
European colonies in, 1:6  
U.S. security policy and interventions, **1:5–9**, 1:6
- AFTAC. *See* Air Force Technical Applications Center (AFTAC)
- Agent Orange, **1:9–10**, 1:181
- AIA. *See* Air Intelligence Agency (AIA); American Institute of Architects (AIA)
- AIDS  
Soviet disinformation on, 1:333  
vaccine research, 3:224
- Airborne Command Post (Looking Glass), **2:237**, 2:238
- Air Combat Command (ACC), 1:12
- Air Commerce Act (1926), 2:2
- Aircraft  
hypersonic and rocket powered, 2:90–92  
Identification Friend or Foe (IFF), 2:98  
intelligence gathering, 1:11–13  
Aircraft carrier, **1:17–20**, 1:18  
Air Force intelligence (U.S.), **1:11–13**, 1:12  
Air Force Office of Special Investigations (AFOSI), **1:13–14**  
Air Force Technical Applications Center (AFTAC), 1:12  
Air Force (U.S.)  
Tethered Aerostat Radar System, 1:94  
Air Intelligence Agency (AIA), 1:12  
Airline security, **1:20–22**, 1:21  
Air marshals, U.S., **1:14–16**, 1:15  
Air plume and chemical detection, **1:16–17**  
Airport security, 1:20–21  
*See also* Airline security
- Air purification  
contamination/decontamination, **1:10–11**, 1:10
- Airships, 1:93  
*See also* balloon flight
- Air technical intelligence, 1:73–76
- Air wings (aircraft carriers), 1:17–18
- Al-Aqsa Martyrs Brigade (Palestine), **1:23**
- Alaskan Pipeline, 2:384
- al-Banna, Sabri, 1:1
- Alberti, Leon Battista (1404–1472), 1:204, 1:227, 1:288
- Albright, Madeleine, 1:325
- Alcohol Tax Unit (ATU), 1:68
- Alex Boncayao Brigade (ABB, Philippines), **1:23**
- Al-Gama'a al-Islamiyya (Islamic Group, IG), **1:23–24**
- Algorithms and data mining, 1:307  
*See also* Ciphers, algorithmic
- Alien Registration Act (1940), 2:251
- ALIR. *See* Army for the Liberation of Rwanda (ALIR)
- Al-Ittihad al-Islami (AIAI), **1:24**
- Al-Jama'a al-Islamiyyah al-Muqatilah bi-Libya, **1:25**
- Al-Jihad, **1:25**
- Al-Kindi, Abu Yusef, 1:226
- Allende, Salvador, 1:29
- Allied Democratic Forces (ADF), **1:26**
- Al-Owhali, Mohamed Rashad Daoud, 2:200
- Al-Qaeda, 1:6, **1:26–27**  
'Asbat al-Ansar funding from, 1:57  
assassinations, 1:61  
in Canada, 1:162  
capture of Khalid Sheikh Mohammed, 1:49  
intelligence on, 3:146  
September 11 attacks on U.S., 3:68, 3:270  
treatment of POWs, 2:125  
USS *Cole* incident, 3:216–217  
wanted poster for leaders of, 1:277
- Al-Qaida. *See* Al-Qaeda
- Al-Zawahiri, Aiman, 1:277
- American Airlines

- hijacked flights—9/11, 3:69  
LAX terminal, 1:27
- American Civil Liberties Union (ACLU), 2:448
- American Communist Party, 2:252–253
- American Federation of Federal Employees (AFGE), 1:77
- American Institute of Architects (AIA), 1:49
- American Media Inc., 1:40
- American Revolution  
espionage and intelligence in, 3:21–23  
guerilla warfare tactics in, 2:74, 3:206
- American Society of Civil Engineers  
WTC tower collapse study, 1:50
- Americas, modern U.S. security policy and interventions, 1:28–31
- Ames, Aldrich H., 1:31–33, 1:196, 2:280–281
- Analytical chemistry, 1:183  
*See also* Chemistry; Forensic chemistry
- Anarchism ideology, 3:148
- Andrea Doria* (aircraft carrier), 1:20
- Angleton, James, 1:202, 2:281
- Anglo-Russian Convention (St. Petersburg, 1907), 2:72
- Angola, 1:8
- Animal research  
adaptations and behaviors derived from genetic, 1:113  
Anthropod-borne Animal Disease Research Laboratory (USDA), 1:109
- ANO. *See* Abu Nidal Organization (ANO)
- Anthrax, 1:33–34, 2:279, 3:214  
American Media Inc. cleanup site, 1:40  
biodetector defense against, 1:111  
as biological weapons, 1:34–37, 1:39–41, 1:43, 2:103  
biotechnology and, 1:36–37  
ease of delivery, 1:36  
in Iraq, 2:165  
military research of, 1:36  
production of, 1:36–37  
reward poster, 1:35  
spores, 3:109–110, 3:244–245  
testing on Gruinard Island, 1:118  
vaccine, 1:37–39, 1:38
- Anthropod-borne Animal Disease Research Laboratory (USDA), 1:109
- Anti-Ballistic Missiles (ABM), 3:120–121
- Anti-Ballistic Missile Treaty (1972), 1:41–42, 3:121
- Antibiotics, 1:43–44  
genomic research in, 2:57–58  
National Pharmaceutical Stockpile Program (NPS), 1:126, 1:319  
resistance to, 1:43, 1:81, 1:82–83, 2:265  
stockpiling of, 1:125
- Anti-drug campaign  
Anti-Drug Abuse Act (1988), 1:362  
Anti-drug advertising, 1:362  
Drug-Free Communities Act (1997), 1:362
- Anti-government groups (U.S.), 3:143–144
- Anti-imperialist Territorial Nuclei (NTA, Italy), 1:44
- Anti-spam legislation, 2:144
- Anti-Terrorism, Crime and Security Act, U.K. (2001), 2:123
- Apartheid, 1:8
- APIS. *See* Advance Passenger Information System (APIS)
- Apollo space program  
need for miniaturized electronics, 2:266  
PNL analysis of lunar materials, 2:394
- Arab-Israeli wars, 2:273
- Arab Revolutionary Brigades. *See* Abu Nidal Organization (ANO)
- ARAC. *See* Atmospheric Release Advisory Capability (ARAC)
- Arbenz Guzman, Pres. Jacobo (Guatemala), 1:29
- Archeology and artifacts  
changing practices of preservation, 1:46  
Holocaust plunder, 1:47  
wartime protection of, 1:45–48  
*See also* Art and antiquities
- Architecture  
building risk assessment software (RAMPART), 1:49  
hidden security checkpoints, 1:50  
structural security and, 1:48–50
- Area 51 (Groom Lake, Nevada), 1:51
- Argentina, intelligence and security, 1:51–53
- Argonne National Laboratory, 1:53, 1:54, 1:111
- Aristide, Pres. Jean-Bertrand (Haiti), 1:30
- Armed Islamic Group (GIA), 1:54
- Arms control  
Conventional Forces Europe (CFE) Agreement, 1:147  
United States Bureau of, 1:55  
*See also* Gun control; Nuclear arms control
- Arms control agreements  
ballistic missiles and nuclear arsenal, 1:76, 1:89  
satellite verification, 3:45
- Arms Export Control Act, 2:155
- Army Field Manual forgery, 1:348
- Army for the Liberation of Rwanda (ALIR), 1:55
- Army Security Agency (ASA, U.S.), 1:56, 2:209
- Army Signal Intelligence Service, U.S. (SIS). *See* Signal Intelligence Service (SIS, U.S. Army)
- Army Signal Security Service, U.S. *See* Signal Intelligence Service (SIS, U.S. Army)
- ARPANet, 2:141
- Arson investigations, ATF, 1:68
- Art and antiquities  
looting of, 1:45–46  
Napoleonic Wars destruction of, 1:46  
Nazi Germany “Great Theft,” 1:47  
repatriation of, 1:46
- ASA. *See* Army Security Agency (ASA, U.S.)
- ‘Asbat al-Ansar, 1:57
- ASG. *See* Abu Sayyaf Group (ASG)
- Ashcroft, John, 2:318
- Asia  
Britain-Russian imperialistic rivalry over, 2:70–72  
IMF focus on, 2:99
- Asilomar Conference, 1:57–58
- Aspin, Secretary. of Defense Les, 1:7–8
- Assassination, 1:58–62  
Al-Qaeda and, 1:60–61  
attempts, 1:60–61  
biochemical techniques, 1:63–64  
biochemical weapons, 1:106–108  
electronic triggers, 1:329  
history of, 1:58, 1:60–61  
mechanical weapons, 1:62–65
- Astronauts, U.S., 2:299
- Asymmetric warfare, 1:68
- ATF (United States Bureau of Alcohol, Tobacco, and Firearms). *See* Bureau of Alcohol, Tobacco, and Firearms (ATF)
- Atmospheric Release Advisory Capability (ARAC), 1:68–69
- Atomic bomb, 2:23
- Atomic emission spectroscopy (AES), 2:24
- Atomic Energy Detection System (USAEDS). *See* U.S. Atomic Energy Detection System (USAEDS)
- ATSA. *See* Aviation and Transportation Security Act (ATSA)
- ATU. *See* Alcohol Tax Unit (ATU)
- Aubisson, Roberto d’, 1:30
- Audio amplifiers, 1:69–70
- Aum Shinrikyo, Aleph, 1:139  
use of nerve gas, 1:36, 1:40–41, 1:64, 3:40  
*See also* Aum Supreme Truth (Aum)
- Aum Supreme Truth (Aum), 1:71  
*See also* Aum Shinrikyo, Aleph
- Australia, intelligence and security, 1:71–72
- Australian Defense Intelligence Organization (ADIO), 1:72
- Austria, intelligence and security, 1:73
- Aviation and Transportation Security Act (ATSA), 1:14, 1:20–21, 1:77, 1:209
- Aviation intelligence  
Air Force intelligence, 1:11–13  
history of, 1:73–76

- Aviation security  
 civil, U.S., **1:209–210**  
 NTSB accident investigations, *2:361*  
 PanAm 103 bombing investigation, *2:399–400*  
 screeners, **1:77–78**, **1:209–210**  
 turbulence detection, *1:364*
- I B I**
- B-2 Bomber, **1:79**  
 B-52, **1:80**  
*Bacillus anthracis*. *See* Anthrax  
 Background investigations, *1:322*  
 Backscatter imaging, *3:53*  
 Bacon, Roger (1220–1292), *1:227*  
 Bacteria  
 aerobic and anaerobic, *1:81*  
 DNA in, *1:80–81*, **1:335–338**  
 identification and classification, *1:81*  
 spore formation, *3:109–110*  
 toxins, *3:166*  
 treatment of, *1:83–84*  
 viral genetics, *1:82–84*, *3:237–239*  
 Bacterial biology, **1:80–85**  
 Bacterial infections  
 antibiotics for, *1:43*  
 antibody formation, *1:81*  
 disease from, *1:83–84*  
 Baghdad Pact, *1:237*  
 Bakunin, Mikhail (1814–1876), *3:150*  
 Ballistic fingerprints, **1:85**  
 Ballistic missile defense (BMD)  
 boost phase intercept, *3:121–122*  
 cruise phase intercept, *3:123*  
 descent phase intercept, *3:123–124*  
 Ballistic Missile Defense Organization (BMDO, U.S.), **1:86**  
 Ballistic missiles, **1:87–91**, *1:87–88*  
 arms control agreements, *1:89*, *2:30*  
 Ghauri (Pakistan), *1:88*  
 Minuteman ICBM (U.S.), *1:87*  
 precision-guided, *2:172*  
 proliferation of, *1:90–91*  
 R-7 ICBM (Soviet Union), *1:89*  
 Balloon flight  
 in Civil War (U.S.), *1:211*  
 first manned flights, *1:91*  
 Hindenburg crash, *1:93*  
 Japanese WWII balloon bombs, *2:34*  
 Montgolfier brothers, *1:92*  
*See also* Airships  
 Balloon reconnaissance, *1:91*  
 Air Force aerostats (blimps), *1:94*  
 history of, **1:91–94**  
 photography, *2:424–425*  
 Project GENETRIX, *1:93–94*  
 Bamford, James, *2:352*  
 El Baradei, Mohamed, *2:139*, *2:161*  
 Barannikov, Victor, *1:148*  
 Barre, Maj. Gen. Mohamed Siad, *1:7*  
 Basque Fatherland and Liberty (ETA), **1:94–95**  
 Bathymetric maps, **1:95–96**  
 Batista, Fulgencio, *1:28*  
 Battle groups (aircraft carriers), *1:17*  
 Baudot code, *1:242*, *2:21*  
 Bauer, Edger (1820–1886), *3:148*, *3:150*  
 Bay of Pigs, **1:96–98**, *1:293*  
 Brigade 2506, *1:97–98*  
 BayTSP  
 copyright laws and, *1:272*  
 Beckwith, Byron De La, *2:8*  
 Beckwith, Col. Charles, *1:322*  
 Belgium, intelligence and security, **1:98–99**  
 Belly buster hand drill, **1:99**  
 Ben-Gurion, David, *2:283*  
 Berlin Airlift, **1:99–101**, *1:100*  
 operations, *1:100–101*  
 Berlin refugees, *1:103–105*  
 Berlin Tunnel, **1:101–103**, *1:102*  
 Berlin Wall, *1:101*, **1:103–106**  
 Brandenburg Gate, *1:104*  
 building of, *1:105–106*  
 Checkpoint Charlie, *1:236*  
 fall of, *1:106*, *1:239*, *1:241*  
 Berman, Howard L., *3:42*  
 Berners-Lee, Tim, *1:171–172*, *2:142*  
 Bernstein, Carl, *1:202*  
 Bernstorff, Count Johann Von, *1:130*  
 Bethe, Hans, *2:246*  
 Bethe carbon cycle, *2:44–45*  
 Bigliarrdo, Roberto Felice, *1:371*  
 Bill of Rights, *2:447*  
 Bin Laden, Osama, *1:6*, *1:277*  
 al-Qaeda, *1:26*, *1:149*  
 'Asbat al-Ansar, *1:57*  
 September 11 attacks on U.S., *3:270*  
 Biochemical assassination weapons, **1:106–108**  
 cyanide, *1:107*, *1:298–299*  
 decontamination from, *1:317–318*  
 detection devices for, *1:143*  
 hemlock, *1:106*  
 poison firing devices, *1:63–64*, *1:65*, *1:107*  
 ricin, *1:107*, *3:24*, *3:166–167*  
 Sidney Gottlieb and the CIA, *1:108*  
 VX nerve agent, *3:246–247*  
 Biocontainment laboratories, **1:108–110**, *1:109*, *3:215*  
 Biodetectors, **1:110–111**  
 Bio-engineered tissue constructs, **1:111–112**  
 Bio-flips, **1:112**  
 Bioinformatics, *2:57*  
 Biological and biomimetic systems, **1:113**  
 Biological and Toxin Weapons Convention, **1:113–114**, *1:116*  
 Biological input/output systems (BIOS), **1:114–115**  
 Biological systems  
 biodetectors, *1:110–111*  
 bio-flip implants for monitoring, *1:112*  
 biomimetic systems, *1:113*  
 Bio-Optical Synthetic Systems (BOSS), *1:121–122*  
 biosensors, *1:117*  
 BioShield Project, *1:122–123*  
 DNA implants into microorganisms, *1:114–115*  
 Life Support for Trauma and Transport (LSAT), *1:120*  
 Personal Status Monitor (PSM), *1:119–120*  
 Biological warfare, **1:115–116**  
 advanced diagnostics, **1:117**  
 anthrax and, *1:33–34*, *1:34–37*  
 biodetectors as defense from, *1:110–111*  
 bioterrorism and, *1:123–125*, *2:103*  
 deterrence strategies to biological warfare, *1:125–126*  
 as security threat, *2:264–265*  
 technology for, *1:174*  
 Biological weapons  
 aflatoxin, *3:166*  
 air, food and water contamination, *1:10–11*, *2:29*  
 anthrax, *1:33–34*, *1:34–37*, **1:39–41**, *1:43*  
 Aum Shinrikyo (Japanese cult), *1:36*, *1:40–41*, *1:64*  
 Biological and Toxin Weapons Convention, *1:113–114*  
 destroyed in Iraq, *1:115*  
 detection of, *1:113*  
 development programs, *1:115–116*  
 diplomatic control of, *1:116*  
 genetic identification of, **1:117–118**, *1:342*, *2:278–279*  
 infectious diseases as, *1:124*, *2:103*  
 Soviet Union test facility, *3:244–245*  
 testing of, *1:118*  
 as weapons of mass destruction, *3:258*  
 zoonoses, *3:286–287*  
 Biology  
 bacterial, *1:80–85*  
*Bergy's Manual*, *1:81*  
 viral, *1:81–82*, *3:236–240*  
 viral classification, *3:236–238*  
 Bio-Magnetics, **1:119**  
 Biomedical technologies, **1:119–120**  
 BioShield Project, *1:122–123*  
 Biometrics, **1:120–121**  
 Biomimetic systems, *1:113*  
 Bio-Optic Synthetic Systems (BOSS), **1:121–122**  
 BIOS. *See* Biological input/output systems (BIOS); Biological systems  
 Biosafety level laboratories (BSL), *1:108–110*  
 Biosensor technologies, **1:122**  
 bio-flip implant research, *1:112*



- detecting biological weapons, 1:117
  - tissue-based, 3:163
- BioShield Project, **1:122–123**
- Biotechnology
  - diagnostic devices, 1:117, 1:120
  - LBL research in, 2:224
  - nanotechnology applications in, 2:295
  - vaccine development, 1:143
- Biotechnology programs
  - detection technologies, 1:110–111, 1:119
- Bioterrorism, **1:123–125**
  - Aum Shinrikyo (Japanese cult), 1:36, 1:40–41, 1:64
  - biological agents and, 1:34–37, 1:124
  - bioterrorism initiative, 1:126
  - Bioterrorism Preparedness and Response Program (BPRP), 1:126
  - CDC disease surveillance as deterrence, 1:170
  - protective measures, **1:125–127**, 2:29, 2:435
- Bishop, Pres. Maurice (Grenada), 1:29
- Bjerkness, Vilhelm, 2:256
- Black chamber, **1:127–128**
- Black ops, **1:128**
- Black September, 1:1, 1:61–62, 2:283–284
  - See also* Abu Nidal Organization (ANO)
- Black Tom explosion, **1:128–130**, 2:6
- Blair, Tony (U.K. Prime Minister), 2:167–168
- Blake, George (British double agent), 1:102
- Bletchley Park, **1:131–133**
  - bombe deciphering machine, 1:131
  - British cryptology operations and cipher school, 1:131–133, 2:21
  - Cairncross and, 1:154
  - Colossus computer, 1:132, 1:138, 1:206, 1:242, 2:21, 3:185
  - Enigma cipher machine, 1:405–407
  - MI6 cryptanalysis and, 2:262
  - Operation Ultra, 3:184–185
  - tight security at, 1:132, 3:184–185
- Blix, Hans, 2:163, 2:164, 2:166, 2:176
- Bludgeons and blunt instruments, 1:64
- Blunt, Anthony, 1:153–154
- BMDO. *See* Ballistic Missile Defense Organization (BMDO, U.S.)
- Bohr, Neils, 2:246, 2:294
- Bolivia, intelligence and security, **1:133**
- Bolland Amendment (War Powers Act), 1:30
- Bolshevik-German conspiracy forgery, 1:345–346
- Bomb
  - canine substance detection, 1:163–165
  - detection devices, **1:135–136**
  - e-bombs, 1:369–370, 1:384
  - JDAM, 2:187–188
  - Bomb damage, forensic assessment, **1:134**
  - Bombe, 1:131, **1:136–138**, 1:206
    - See also* Bletchley Park
  - Bonaparte, Charles, 2:6
  - Bonaparte, Napoleon, 2:296–298, 3:127
    - British assassination attempts on, 2:297
  - Booster rockets, 1:90
  - Border and Transportation Security, DHS Directorate of (BTS), 1:44–45, 2:440
    - Border Patrol, U.S., 2:94
    - fingerprint identification systems, 2:19, 2:95
    - INSPASS (Immigration and Naturalization Service Passenger Accelerated Service System), **2:115–116**
    - Port Passenger Accelerated Security System (PORTPASS), **2:439–440**
  - Border security
    - Border Patrol, U.S., 2:94
    - Customs Service, U.S., 1:296–297
    - International Border Interdiction Training, 1:297
  - Bosnia and Herzegovina
    - intelligence and security, **1:138–139**
    - NATO Stabilization Forces in, 1:138
  - Botulinum toxin, **1:139**
  - Botulism. *See* Botulinum toxin
  - Boyd, Belle, 1:211–212, 1:416
  - Bracy, Arnold, 3:75
  - Brady, James, 3:56
  - Brain-machine interfaces, **1:140**
  - Brain wave scanners, **1:141**
  - Brazil
    - aircraft carrier development, 1:19
    - intelligence and security, **1:141–142**
  - Brenner, Sydney, 2:53
  - Brezhnev, Leonid (Soviet president), 1:166
    - death of, 1:240
    - Soviet economy, 1:239–240
    - Strategic Arms Limitation Talks (SALT), 1:238
  - Brigade 2506 (Bay of Pigs, Cuba), 1:97–98
  - British Columbia Cancer Agency
    - SARS genome sequencing, 1:250
  - British intelligence
    - Cambridge University Spy Ring, 1:151–155
    - cryptology operations and cipher school, 1:131–133
    - MI5 (British Security Service), 2:260–261
    - MI6 (British Secret Intelligence Service), 2:262
    - Profumo affair with Soviet informant, 1:154
    - Room 40 cryptography (WW I), **3:28**
  - British Terrorism Act, **1:142**
  - Brogie, Louis de, 2:271, 2:295
  - Brookhaven National Laboratory, **1:143–144**, 1:143
    - Mini-Ramen LIDAR System (MLRS), 1:143
  - Brown, Ron, 1:246
  - Brzezinski, Zbigniew (U.S. security advisor), 1:7, 1:166, 2:358
  - BTS. *See* Border and Transportation Security, DHS Directorate of (BTS)
  - Bubonic plague, **1:144–145**, 2:279
  - Bucher, Lloyd M, 2:456
  - Budget and Accounting Act (1941), 2:48
  - Bugs (microphones) and bug detectors, **1:145–147**
    - Egyptian embassy, 1:404–405
    - noise generators, 2:341
    - parabolic microphones, 2:403
    - wiretaps and surveillance act restrictions, 2:31–32
    - See also* Listening devices
  - Bundy, McGeorge, 2:189, 2:198, 2:358
  - Bureau of Alcohol, Tobacco, and Firearms (ATF), **1:66–68**
    - ballistic fingerprint matches, 1:85
    - bomb damage assessment, 1:134
  - Bureau of Arms Control (U.S.), **1:55**
    - Biological and Toxin Weapons Convention, 1:113
  - Bureau of Diplomatic Security, U.S., **1:330**
  - Bureau of Industry and Security, U.S. (BIS), 1:246
  - Bureau of Intelligence and Research (INR) U.S. State Dep't, **1:323–324**
  - Burgess, Guy, 1:153
  - Bush, George H.W.
    - as CIA director, 1:196, 1:310
    - Panama intervention, 1:30, 1:279
    - Persian Gulf War, 1:147
    - U.S. and Russia announces testing moratorium, 1:254
  - Bush, George W., 1:194
    - Antiballistic Missile (ABM) Treaty, 1:42
    - at Argonne National Laboratory, 1:54
    - BioShield Project, 1:123
    - national security policy, 1:148–150
    - 9/11 terrorist attacks, 1:148, 3:70–71
    - United Nations and Iraq disarmament, 2:163–167
    - Voice of America, 3:243
    - war on terrorism, 3:71–72
  - Bush administration (1989–1993)
    - National Security Council, 2:358–359
    - National Security Directive, 1:147
    - national security policy, **1:147**
    - Somalian relief and Mogadishu debacle, 1:7–8
  - Bush administration (2001–)
    - Antiballistic Missile (ABM) Treaty, 1:42
    - National Security Council, 2:359
    - national security policy, **1:148–150**
    - 2002 National Security Strategy, 2:310–311

- pre-emptive strike doctrine, 1:149–150
- Saddam Hussein and Iraq, 2:166, 2:173–176
- war on terrorism, 1:279, 3:71–72
- ## ICI
- Cadore letter forgery, 1:344
- Cailliau, Robert (WWW co-creator), 1:171–172
- Cairncross, John, 1:154
- Caller ID, **3:137–138**
- Cambodia
- communist capture of the Mayaguez, 2:30
  - Freedom Fighters, **1:151**
- Cambridge University Spy Ring, **1:151–155**, 2:203, 2:261, 3:96
- defections of, 1:153
  - Michael Straight and Anthony Blunt, 1:154
- Cameras, **1:155–157**
- concealment of, 1:157–158, 1:265–266
  - copy, 1:156–157
  - digital, 2:423
  - disguising, 1:159
  - infra-red, 1:390
  - miniature, **1:157–160**, 1:265–266
  - robot camera (German), 1:156
- Camouflage and concealment
- concealment devices, 1:265–267, 1:266
  - passive methods, 1:157–158, 1:265
- Canada
- Canadian Security Intelligence Agency (CSIS), 1:160, 1:161–163
  - counter-terrorism policy, **1:160–161**
  - intelligence and security, **1:161–163**
  - NORAD (North American Air Defense Agreement), 2:344–346
  - October Crisis of 1970, 1:160
  - Resolution 1373 (U.N. Security Council), 1:160–161
  - Royal Canadian Mounted Police (RCMP), 1:161, 1:363
  - terrorism in, 1:160, 1:162
- Canaris, Wilhelm, 1:2–3, 2:64
- Canine substance detection, **1:163–165**
- Carcinogens, 1:5, 3:166
- Carlucci, Frank, 2:358
- Carroll, Joseph, 1:13
- Car security, LoJack and GPS, 2:69
- Carter, James E., 1:166, 1:167
- CIA surveillance restrictions, 1:203
  - Iranian hostage crisis, 1:166
  - Shah of Iran and hostages, 2:159–160
  - Somalia agreements, 1:7
- Carter administration (1977–1981)
- cut aid to dictatorships, 1:29
  - National Security Council, 2:357–358
  - national security policy, **1:165–167**
  - openness policy, 1:279
  - Somalia agreements, 1:7
- Casey, William J., 1:196, 1:311
- Castilla Armas, Carlos, 1:29
- Castro, Fidel, 1:28, 1:29
- Bay of Pigs, 1:96–98, 1:293, 2:198
  - CIA disruption attempts, 2:387–388
  - Soviet missile deal (missile crisis), 1:293–295
- CBIRF. *See* Chemical and Biological Incident Response Force (CBIRF)
- Census Bureau, 1:245–246
- Center for the Study of Intelligence (CSI, CIA), **1:196–197**
- Centers for Disease Control and Prevention (CDC), **1:168–170**, 2:455
- branch of HHS, 2:81
  - cost study of disease outbreaks, 2:104
  - economic and bioterrorism report, 1:36
  - protective measures development, 1:126
  - SARS genomic map, 1:250
- Central Asia
- Britain-Russian imperialistic rivalry over, 2:70–72
- CERN, **1:170–172**
- Berners-Lee and the World Wide Web, 1:171–172, 2:142
  - particle physics and accelerators, 1:170–171
- Chad, oil revenue economic controls, 1:9
- Chadwick, Sir James, 2:246
- Chamora, Violeta, 1:30
- Charged coupling devices (CCD), 2:422
- Charles de Gaulle* (aircraft carrier), 1:20
- Charles' Law (atmospheric gases), 2:258
- Chechen-Russian conflict, **1:172–173**
- Chechnya (Russian republic), 1:172–173
- Russian-Chechen referendum, 1:173
  - Russian troops in, 1:173
  - Stalin's mass deportation from, 1:172
- Chemical analysis, 1:184–185
- Chemical and Biological Defense Information Analysis (CBIAC), **1:174**
- Chemical and Biological Incident Response Force (CBIRF), **1:176–177**, 1:179
- Chemical and Biological National Security Program (CBNP), 2:339–340
- Chemical and biological science and technology
- analysis of manufacturing processes, 1:174
  - detection technologies, **1:175–176**
- Chemical-biological mass spectrometer (CBMS), 2:179, 2:381
- Chemical Safety and Hazard Investigation Board (USCSB, U.S.), **1:177–178**
- Chemical safety and response
- accidental release of chemicals, 1:177
- Chemical and Biological Incident Response Force (CBIRF), 1:176–177, 1:179
- Chemical Safety and Hazard Investigation Board (USCSB, U.S.), 1:177–178
- detection technologies, 1:175–176
- emergency responses, **1:178–179**
- federal assistance, 1:179
- state and local emergency response commissions, 1:178–179
- Chemical warfare, **1:180–183**
- chemical agents used, 1:181–183, 2:321–322
- Chemical and Biological Incident Response Force (CBIRF), 1:176–177
- radiological, 1:171
- Chemical warfare response teams, 1:182
- Chemical and Biological Incident Response Force (CBIRF), 1:176–177
- Chemical Biological Incident Response Force (U.S. Marines), 1:176–177
- Chemical weapons
- Geneva Protocol (1925) ban on, 1:180–181
  - Iraq's use of, 1:176, 1:298, 1:319, 2:165
  - mustard gas, 2:290–291
  - nerve gases, 2:321–322
  - in Vietnam war, 1:181
  - as weapons of mass destruction, 3:258
  - in World War I, 1:180–181, 3:272–273
- Chemistry
- analytical, 1:183
  - applications for intelligence community, **1:183–185**
  - forensic, 1:183, 1:338, 2:37
  - separation methods, 1:183–184
- Chernobyl nuclear power plant accident, **1:185–188**, 1:186, 2:24
- satellite imagery of, 1:187
- Chiang Kai Shek (Taiwanese leader), 1:233, 3:134
- Children's Television Act, 2:10
- Chile
- aircraft carrier development, 1:19
  - intelligence and security, **1:188–189**
  - intervention in, 1:29
  - political dissidents treatment in, 1:188
- China
- aircraft carrier development, 1:19–20
  - copyright in, 1:190
  - civil war in, 1:233
  - formation of People's Republic of China (PRC), 2:208
  - intelligence and security, **1:189–190**
  - looting of historical artifacts, 1:46
  - Nixon's visit to, 2:335
  - Severe Acute Respiratory Syndrome (SARS), 1:248–252



- Tachen Straits crisis, 1:237
- United Nations Security Council and, 1:189
- U.S. satellite technology exports to, 3:41–42
- U.S. warhead designs in, 1:190
- Chinese espionage
- Cox Report (U.S.), 1:191
- interest in U. S. technology, 1:191, 1:365, 2:133
- in U.S., **1:190–191**
- Cholana Kangtoap Serai Cheat Kampouchea. *See* Cambodia, Freedom Fighters
- Christopher, Warren, 1:217
- Chromatography, 1:184
- gas, 1:175, 2:38
- thin layer, 2:38, 3:161–162
- Church, Sen. Frank (U.S.), 1:62, 1:107, 1:192, 1:201, 1:203, 3:66
- Church Committee, 1:107, **1:192–193**, 1:194
- CIA legal restrictions, 1:201, 1:203, 1:279
- congressional oversight of intelligence community, 1:194, 2:135–136
- surveillance act passed following report, 2:31
- Churchill, U.K. Prime Minister Winston, 1:231, 1:233, 3:106
- CIA administration
- authority lines and directorates, 1:195, 3:203
- directors (DCI), 1:308–312, 3:203–204
- funding for data mining research, 1:307
- intelligence for U.S. President, 2:444–445
- legal restrictions on, **1:202–203**, 1:279
- CIA (Central Intelligence Agency), **1:193–196**, 3:203
- assassination attempts and restrictions, 1:62, 1:194, 1:203
- Bay of Pigs (Cuba), 1:293
- Berlin Tunnel, 1:101–103
- careers in, 2:119–120
- Cold War operations, 1:232
- double agents, 1:31–33, 1:102, 1:360–361
- George H.W. Bush, Director of, 1:147
- Project GENETRIX canceled, 1:94
- publication of training manuals, 1:30
- response to spy ring defections, 1:154
- Sidney Gottlieb and biochemical weapons, 1:108
- CIA covert operations, 1:277
- Delta Force, Middle East and, 1:323
- dirty tricks, 1:331
- Glomar Explorer* -Soviet submarine salvage, 2:66–67
- Iran-Contra affair, 1:30, 1:279, 2:155–157
- Operation Mongoose (Cuba), 2:387–388
- secret Asian wars, 1:196
- training and indoctrination for, 1:277–278
- in Vietnam War, 1:279
- Watergate break-in, 1:202
- CIA directorates and services, 1:201, 1:311
- Center for the Study of Intelligence (CSI), **1:196–197**
- Directorate of Science and Technology (DS&T), **1:197–198**
- Foreign Broadcast Information Service, **1:198–199**
- guerilla warfare training base, 1:234
- CIA formation and history, 1:195–196, **1:199–201**, 1:200
- growth of, 1:200–201
- CIA Information Act (1984), 1:203
- CIAO. *See* Critical Infrastructure Assurance Office (CIAO)
- CIG (Central Intelligence Group), 1:200
- CIPA. *See* Classified Information Procedures Act (CIPA)
- Cipher disks and wheels, **1:204**, 1:205
- in Civil War (U.S.), 1:211
- Cipher keys, **1:204–205**
- algorithmic, 1:218, 1:225, 1:286–287, 1:319
- mobile phone, 2:73
- public, 1:227–228
- RSA algorithm, 1:287–288, 1:291, 2:446
- Cipher machines, **1:205–207**
- Colossus computer, 1:132, 1:138, 1:206, 1:242, 2:21, 3:185
- digital computers as, 1:206
- Egyptian embassy cipher room bugged, 1:404–405
- Geheimschreiber, 1:205–206, 2:21
- one-time tape system, 1:207
- Playfair system, 1:289, **2:426**
- Purple machine (Japanese), 2:459–460, 3:185
- rotor-based Enigma type, 1:205, 1:206
- Signal Intelligence Service (SIS, U.S. Army), 1:243–244, 2:386–387
- Typex, **3:177**
- See also* Cryptography
- Cipher pad, **1:207–208**, 1:291
- Ciphers
- ADFGX Cipher, 1:3–4, 1:205, 1:290
- algorithmic, 1:218, 1:225, 1:228, 1:286–287
- block, 1:227
- Lorenz cipher, 1:137, 1:242, 2:21
- Polybius square, 1:3–4, 1:288
- public key, 1:227–228
- stream ciphers, 1:208, 1:227
- substitution cipher, 1:205, 1:226, 1:405
- SZ42 Cipher, 1:205
- See also* Cryptography
- CIPRIS. *See* Coordinating Interagency Partnership Regulating International Students (CIPRIS)
- Civil defense
- homeland security and, 2:85–86
- Civil Liberties Act (1988), 2:122
- Civil rights and liberties
- Habeas Corpus Act (1863), 2:121–122
- Patriot Act and, 1:386–387
- Soviet propaganda prompted civil rights legislation, 2:450
- Civil Rights Commission, U.S., **1:247–248**
- Civil rights movement
- Civil Liberties Act (1988), 2:122
- Civil Rights Act (1957), 1:247, 2:7–8
- COINTELPRO illegal operations discrediting groups, 1:229–230
- FBI investigation of assassinations, 2:8
- Civil War (U.S.)
- Balloon reconnaissance, 1:91, 1:92
- cipher disk used in, 1:204
- espionage and intelligence in, **1:210–212**, 3:206–207
- uncontrolled borders, 1:210
- women spies in, 1:211
- Clark, John (18th century), 3:22
- Clark, William, 2:358
- Clarke, Richard (security advisor), 1:299
- Classified information, **1:213–216**
- access to, 3:60–61
- declassification of, 1:215–216
- Classified Information Act (1980), 2:135
- Classified Information Procedures Act (CIPA), 1:213–214, 1:259
- Classified National Security Information Act, 1:214–215
- Clean Air Act
- 1990 amendment, 1:177
- Cleopatra (Egyptian Queen), 1:106
- Clifford, Clark, 2:189, 2:355
- Clinton, William J., 1:17, 1:217
- Haiti intervention, 1:30
- ISAC concept by, 1:301
- signs Comprehensive Test Ban Treaty (CTBT), 1:254
- Vietnam War influence on, 1:216–217
- Clinton administration (1993–2001)
- alleged Chinese campaign donations to, 1:190, 3:41
- counter-terrorism policy, 1:176, 3:145–146
- declaration against terrorism after Khobar Towers bombing, 2:204
- foreign aid policy, 1:217
- National Security Council, 2:359
- national security policy, **1:216–218**
- openness policy, 1:279

- Presidential review directive (PRD), 1:217
- U.S. satellite technology exports to China, 3:41–42
- Clipper chip, **1:218**
- Closed circuit television systems (CCTV), 1:156, **1:219–221**
- Cloud seeding, 2:257, 2:259–260
- Coast Guard, U.S., **1:221–222**
- coordinating gov. agencies roles in homeland security, 1:222
  - National Maritime Intelligence Center, 2:336–337
  - National Response Center, **1:223**
  - National Response Team, 2:306–307
  - port security, 2:437–438
  - Port Security Units (PSUs), 2:438
- Cockpit voice recorders, 2:26
- Code-breakers, 1:127–128
- Code names, **1:223–224**
- Codes and ciphers, **1:224–228**
- in American revolution, 3:22–23
  - code types, 1:227, 1:242
  - fast and scalable scientific computation of, **1:228–229**
  - French resistance coded messages, 2:42–43
  - German code books captured by British, 3:274–275
  - Morse code, 1:225
  - See also* Ciphers
- Code-talkers (Navaho Indians), 1:291, 3:263–265
- Code words, **1:224**
- CODIS. *See* Combined DNA Index System (CODIS)
- Coherent scattering, 3:53
- COINTELPRO, 1:229–230
- Colby, William E., 1:192, 1:196, 1:310
- Cold fusion, 2:45
- The Cold War
- aerial reconnaissance in, 1:75–76
  - beginnings of, **1:230–232**
  - Berlin blockade by Soviet Union, 1:99–101, 1:103
  - Berlin Wall, 1:103–106, 1:239, 1:241
  - capitalism vs. socialism, 1:232, 1:233
  - Cold War History Project, 1:332–333
  - development of CIA in, 1:200
  - end of, 1:241
  - KGB operations during, 2:201
  - Nixon's arms reduction talks, 1:238
  - Pres. Truman on, 1:231–232
- The Cold War (1950–1972), **1:233–238**
- The Cold War (1972–1989): the collapse of the Soviet Union, **1:238–241**
- Colladen, Daviel, 3:90
- Colombia, intelligence and security, **1:241–242**
- Colossus computer (1rst programmable computer), 1:132, 1:138, 1:206, **1:242–243**, 2:21, 3:185
- Combat aircraft
- B-2 Bomber, 1:79
  - B-52 Bomber, 1:80
  - balloons use as, 1:92–93
  - F-117, 2:1, 3:116
  - in Soviet Union, 1:75
- Combined DNA Index System (CODIS), 1:336
- Commerce Department, U.S. (DOC)
- Critical Infrastructure Assurance Office (CIAO), 1:282–283
  - intelligence and security, **1:245–246**
- Commissar Order (Nazi Germany), 1:3
- Communicable diseases
- Federal quarantine legislation, 1:250
  - isolation and quarantine, **1:248–252**
- Communication satellites, 1:364
- Communications Satellite Act, 2:10
- licensing of, 3:42
- Communications intelligence (COMINT), **1:243–244**
- telegraph intercepts during Spanish-American War, 3:102–103
- Communications policy
- Children's Television Act, 2:10
  - Communications Act (1934), 2:10
- Communication systems
- diplomatic secure international, 1:252
  - national security and emergency preparedness, **1:252**
- Communism
- in African countries, 1:7–8
  - American Communist Party, 2:252–253
  - anti-communism hysteria, 2:122–123
  - Cold War infiltration of, 1:233
  - FBI domestic efforts against, 2:7
  - Middle East—U.S. defense against, 1:237
  - U.S. Communist Party and Palmer raids, 2:122
  - U.S. resistance to, 1:201, 1:279
- Comprehensive Nuclear Test Ban Treaty Organization, 1:254
- Comprehensive Test Ban Treaty (CTBT), **1:253–254**, 2:394, 3:64
- ratification of, 1:254
- Compton, Arthur H., 1:370
- Compton effect (EMP), 1:370
- Computer Abuse and Amendments Act (1994), 1:256
- Computer-aided design (CAD), 1:259
- Computer Assisted Passenger Prescreening System (CAPPS), 2:123–124, 3:72
- Computer Conservation Society (U.K.)
- preservation of Colossus cipher computer, 1:132, 1:138, 1:206, 1:242, 2:21, 3:185
- Computer crimes
- cyber-security Enhancement Act (2002), 1:256
  - hackers and, 1:255–256, 1:256–257
  - Pentagon attack, 1:256
- Computer data and documents
- access authorization for, 1:263
  - backups for security, 1:300
  - degausser, 1:343
  - digital signatures, 1:262
- Computer Fraud and Abuse Act (1986), **1:255–256**, 2:302
- Computer hackers, **1:256–257**
- exposing computer security flaws, 1:256–257, 1:300
- Computer hardware
- security of, **1:257–258**
  - supercomputers, 3:128
  - theft prevention, 1:262
- Computer keystroke recorder, **1:258–259**
- Computer modeling, **1:259–260**
- Computer networks
- Echelon, 1:370–372
  - wireless, 1:300
- Computer Security Act (1987), **1:261**
- Computer Security Division (NIST), **2:333–334**
- Computer software
- anti-virus, 1:261–262, 2:105
  - building risk assessment software (RAMPART), 1:49
  - data encryption, 1:262, 1:289, 1:291
  - data mining, 1:307
  - Image processing, 3:13–14
  - Internet surveillance, 2:146
  - modeling, 1:259–260
  - name recognition, 2:94
  - Pretty Good Privacy (PGP), 1:228, 1:287, 1:291
  - security of, **1:261–263**
  - simulations and war games, 1:259–260
  - virtual reality modeling language (VRML), 1:259
- Computer systems
- Computer Security Act (1987), 1:261
  - data destruction, **1:255**
  - firewall software for, 1:263, 1:300
  - fraud and abuse of, 1:255–256
  - hardware security, 1:257–258
  - local networks, 1:258
  - new technologies, 3:128
  - security, 1:256–257, 2:8
- Computer tomography (CT scanners), 1:22, 1:135–136, 3:52
- Computer viruses, **1:263–265**
- anti-virus software and, 1:261–262, 2:105
  - hackers and, 1:256, 1:300
  - ILOVEYOU virus, 1:263, 1:264
  - macro viruses and malicious data, 2:245
  - NIPC and "Love Bug" virus, 2:112–113
  - trojan horse programs, 1:300
- Concealment devices, **1:265–267**
- doo transmitter, 1:359
- Congo
- civil war, 1:6

- Congress, U. S.  
   Joint House-Senate Intelligence Committee, 2:129  
   oversight of intelligence community, 2:130, **2:135–136**  
   *See also* Church Committee; Pike Committee
- Conner, R.D.W., 2:300
- CONPLAN (counter-terrorism policy), 3:145–146
- Constitutional law and privacy rights, 2:447–448
- Consumer Information Center, 2:51
- Consumer Product Safety Act (1972), 1:267
- Consumer Product Safety Commission (CPSC), **1:267**, 1:268
- Consumer Sentinel Network, 2:97
- Contamination / decontamination  
   air and water security issues, 1:10–11  
   *See also* Decontamination methods
- Continuity Army Council, 1:267
- Continuity Irish Republican Army, **1:267–268**
- Continuity of Government (U.S., COG), **1:269–270**  
   Department of Homeland Security changes to, 1:269–270  
   Mount Weather, 2:285–286
- Continuous Assisted Performance (CAP), **1:270**
- Coordinating Interagency Partnership Regulating International Students (CIPRIS), 2:114
- Coordinator for Counter-Terrorism, (U.S. Dept. of State), **1:270–271**, 1:271
- COPS (Community Oriented Policing Services), 2:194, 2:221
- Copyright laws  
   BayTSP and, 1:272  
   Copyright Act, U.S., 1:271  
   Digital Millennium Copyright Act (DMCA), 1:272  
   security, **1:271–272**
- Coral Sea, battle of the, 1:19
- Corporate espionage, 1:255–256
- Cospass-Sarsat satellite system (NOAA), 2:341
- Counter-espionage  
   economic espionage, 1:373  
   U.S. and U.K. response to spy ring, 1:154
- Counterfeit currency  
   Counterfeiter profiles, 1:273  
   technology and manufacture of, 1:273, 1:273–274  
   technology preventing, 1:274
- Counterfeiter profiles, 1:273
- Counter-intelligence, **1:274–275**  
   agents, 1:275  
   CIA and, 1:194  
   COINTELPRO, 1:229–230  
   double agents, 1:275  
   FBI measures for, 2:7, 2:8
- National Counterintelligence Policy Board, 1:324  
   NCIX office, 2:317–318  
   procedures investigation, 1:32–33
- Counter-intelligence Center (CIC, CIA), 1:274
- Counter-measures  
   electronic, 1:387–388
- Counter-terrorism  
   CONPLAN, 3:145–146
- Counter-terrorism agencies  
   Coordinator for Counter-Terrorism, (U.S.), 1:270–271, 3:200–201  
   Counter-terrorism Rewards Program, 1:276, 1:277  
   DCI Counter-terrorist Center, 3:201  
   Security, Infrastructure Protection and Counter terrorism, U.S. National Coordinator, 3:62  
   Special Operations Command, 3:200
- Counter-terrorism efforts  
   Austrian financial intelligence, 1:73  
   biodetectors, 1:110–111  
   Brookhaven National Laboratory, 1:143–144  
   CIA and, 1:201  
   FBI and, 2:8–9, 3:201  
   Los Alamos National Laboratory and, 2:240–241  
   Special Elite Anti-terrorism Force (Bolivia), 1:133  
   Terrorist Threat Integration Center, 1:149
- Counter-terrorism operations  
   Argonne National Laboratory, 1:53  
   Delta Force, 1:322–323  
   Operation Liberty Shield, 2:385–386  
   Sudan and Afghanistan attacks, 2:274
- Counter-terrorism policy  
   Clinton and, 1:176  
   deterrence, 3:199–200  
   food supply protection, 2:29  
   United States, 3:198–201
- Counter-terrorism Rewards Program, **1:276**, 1:277  
   part of Rewards for Justice Program, 1:276
- Covert operations, **1:276–279**  
   dirty tricks, 1:331  
   training and indoctrination for, 1:277–278
- CPSC. *See* Consumer Product Safety Commission (CPSC)
- Cray, Seymour, 3:128
- Cray supercomputers, 3:128
- Crib analysis, **1:280**
- Crick, Francis, 2:53
- Crime prevention  
   intelligence agencies aiding, **1:280–281**  
   liberal democracies and crime rate, 1:281
- Crime rate trends, 2:194–195
- Criminal Investigation Division (IRS), 2:138
- Criminal profiling, 2:449
- Crisis Relocation Facilities, 1:269
- Critical infrastructure, **1:282**  
   Critical infrastructure Assurance Office (CIAO), **1:282–283**  
   Information Security, U.S. Office of, 2:106
- Croatia, intelligence and security, **1:284**
- Cruise missiles, **1:284–285**
- Cryptanalysis  
   Arab invention of, 1:226–227, 1:288  
   breaking of Japanese naval codes (WWII), **3:285–286**  
   crib, 1:280  
   methods of, 1:228  
   NSA involved in, 2:352–353  
   Signal Intelligence Service (SIS, U.S. Army), 1:243–244, 2:386–387  
   use in Korean war, 2:209
- Cryptography  
   cipher machines, 1:205–207  
   codes and ciphers, 1:224–228, 1:395  
   declassified documents, 1:216  
   DNA encoding, 1:341–342, 2:265  
   information security, 2:105–106  
   number theory and, **1:286–287**  
   quantum, 1:208, 1:228, 2:295, 2:462  
   stream-cipher technique, 1:205  
   *See also* Cipher machines; Ciphers; Codes and Ciphers
- Cryptography computers and software  
   Colossus computer (1st programmable computer), 1:132, 1:242–243  
   computer simulations, 1:228–229  
   Pretty Good Privacy (PGP), 1:228, 1:291  
   scalable algorithms, 1:229  
   *See also* Cipher machines
- Cryptography history, **1:287–291**, 1:288, 1:289  
   in American revolution, 3:22–23  
   Arab scholars and, 1:226–227, 1:288  
   black chamber and code-breakers, 1:127–128  
   in Civil War (U.S.), 1:211, 1:289  
   Egyptian hieroglyphics, 1:288  
   Enigma cipher machine, 1:131–132, 1:205, 1:206, 1:291, 1:405–407  
   Geheimschreiber cipher machine (WWII Germany), 1:205–206, 2:21  
   radio's influence on, 1:290  
   telegraph and, 1:419  
   in World War I, 1:290–291, 3:28, 3:272  
   in World War II, 3:281
- Cryptonyms, **1:291–292**
- CTBT. *See* Comprehensive Test Ban Treaty (CTBT)
- CT scanners, 1:22, 3:52
- Cuba, 1:29, **1:293–295**  
   CIA activities in, 1:201  
   independence of, 1:28

- intelligence and security, **1:292–293**  
 Soviet signals intelligence in Lourdes, 3:95  
 Spanish-American War, 3:101–103
- Cuban Missile Crisis, **1:293–295**  
 Kennedy communications during, 1:252  
 missile site in, 1:196, 1:294  
 operations against U.S., 1:292
- Cult of Assassins, 1:60
- Currency, U.S., 3:170  
 monetary policy and supply, 2:12–13  
 printing of, 1:403–404
- Customs Service, U.S., **1:296–297**  
 Operation Green Quest, 1:296  
 Project Shield America, 1:296–297
- CWIN. *See* Cyber Warning Information Network (CWIN)
- Cyanide, 1:107, **1:298–299**
- Cyber security, **1:299–301**  
 breaching of, 1:300–301  
 Cyber-security Enhancement Act (2002), 1:256  
 Cyber Security Research and Development Act (2002), 1:299
- Cyber Warning Information Network (CWIN), **1:301–302**
- Czechoslovakia  
 communism in, 1:232  
 intelligence and security, **1:302–303**
- DI**
- D notice (defense notice), **1:305**
- Daley, William, 1:246
- Dancer, John, 2:267
- Daniken, Erik von, 2:453
- DARPA (Defense Advance Research Projects Agency), **1:305–306**  
 Advanced Diagnostics Program, 1:117  
 ARPA computer network, 1:252, 1:306, 2:141  
 biomedical programs, 1:113, 1:114–115, 1:119–120  
 biotechnology programs, 1:119, 1:121–122, 1:122  
 brain-machine interfaces for robotics, 1:140  
 Continuous Assisted Performance (CAP), 1:270  
 Internet, dynamic and static addresses, **2:143**  
 rover race, 1:306  
 space research programs, 1:306  
 tissue engineering, 1:111–112
- Daschle, U.S. Sen. Tom, 1:214
- Data encryption, **1:395–396**  
 software, 1:262, 1:289, 1:291
- Data Encryption Standard, 1:207, 1:289, 1:291, 1:396
- Data mining, **1:307–308**, 1:308
- Dead drop spike, **1:315**
- Dead letter box, **1:315–316**
- Debs, Eugene V. (1855–1926), 2:122
- Decontaminants, 1:317–318
- Decontamination methods, **1:316–319**, 1:317  
 chemical methods, 1:317–318  
 detoxification from mustard gas, 2:291  
 gaseous treatments, 2:244–245  
 military treatment facilities, 1:317–318  
 physical methods, 1:316–317  
 radiation, 2:244  
 ultra-high pressure sterilization, 2:244  
 U.S. mail, 2:244–245
- Decryption, **1:319–320**  
 Bletchley Park and, 1:131–133  
*See also* Cryptanalysis
- Defense industry simulations from entertainment industry, 1:259–260
- Defense Information Systems Agency, U.S (DISA), **1:320**
- Defense Intelligence Agency, United States  
 sections and directorates, 1:328–329
- Defense Intelligence Agency, United States (DIA), **1:327–329**  
 remote viewing experiments, 2:452
- Defense Meteorological Satellite Program (DMSP), 2:340–341
- Defense Nuclear Facilities Safety Board (DNFSB), U.S., **1:321**
- Defense Security Service, U.S., **1:321–322**
- Defense Support Program satellites (DSP), 3:47–49
- De Lome letter forgery, 1:344
- Delta Force, **1:322–323**
- Democratic National Committee  
 Chinese contributions to, 1:190–191
- Department of Defense (DOD), 1:252, **1:350–353**  
 bio-flip implant research, 1:112  
 BMDO, 1:86  
 Chemical and Biological Defense Information Analysis (CBIAIC), 1:174  
 Defense Information Systems Agency, U.S (DISA), 1:320  
 dual use technology, 1:364–365  
 history of, 1:350–351  
 intelligence agencies in, 3:204  
 leadership and commands, 1:352–353  
 NASA joint programs with, 2:298–299  
 resources of, 1:351–352
- Department of Energy (DOE), 1:53, **1:353–356**  
 Atmospheric Release Advisory Capability (ARAC), 1:68–69  
 comprehensive energy plan, 1:354  
 Department of Energy Organization Act (1977), 1:354  
 Nuclear facilities safety board, 1:321  
 programs and offices, 1:354–356
- Department of Health and Human Services (U.S.)  
 bioterrorism initiative, 1:126
- Department of Homeland Security, 3:71  
 Operation Liberty Shield, 2:385–386
- Desch, Joe, 1:137
- De Souza, Steven E. (screenwriter), 1:259–260
- DEST. *See* Domestic Emergency Support Team (DEST)
- Detection technologies  
 biotechnology programs, 1:110–111, 1:119  
 bombs, 1:135–136  
 chemical and biological, 1:175–176, 3:260–263  
 Los Alamos National Laboratory, 2:239–241  
 metal detectors, 2:254–256  
 nuclear, 2:240, 3:260–262  
 PNNL research in, 2:395  
 polymerase chain reaction (PCR), 1:117, 2:56, 2:379, 2:433–436  
 radiation detector, 1:144  
 sensor development, 1:143  
 sniffer dogs, 1:163–165  
 solid-phase micro extraction techniques, **3:89**  
 X-ray machines, 1:175
- Deutch, John M., 1:196, 1:311
- Deuterium, 2:81–82, 2:247
- Dewey, George, 3:102–103
- Dexamphetamine “go” pills, 1:270
- Dial tone decoder, **1:329**
- Digital Encryption Standard, 1:227
- Digital Globe, 3:44
- Digital Millennium Copyright Act (DMCA), 1:272
- Digital photography, 2:422–423  
 cameras, 2:423  
 charged coupling devices (CCD), 2:422  
 encrypted watermarking, 2:423  
*See also* Cameras; Photography
- Digital signatures, 1:262, 2:446
- Directed energy weapons  
 Radio frequency (RF) weapons, 3:5–6  
 space-based, 3:122
- Directorate of Science and Technology (DS&T, CIA), **1:197–198**, 1:201  
 psychic “remote viewing” of sites, 1:198
- Director of Central Intelligence (DCI), **1:308–312**, 2:444–445, 3:203–204
- Dirty tricks, **1:331**  
 Egyptian embassy cipher room bugged, 1:404–405
- DISA. *See* Defense Information Systems Agency, U.S (DISA)
- Disaster relief  
 Disaster Relief Act (1974), 2:15



- See also Federal Emergency Management Agency (FEMA)
- Disinformation campaigns, **1:331–324**, 2:450
- DNA detection and identification  
 biological weapons, 1:342  
 DNA signatures, 1:342  
 Human Genome Project, 2:265  
 of humans, 1:337, 1:341, 2:36–37, 2:37  
 hybridization assays, 1:339, 1:339–340  
 polymerase chain reaction (PCR), 1:117, 2:56, 2:379, 2:433–436  
 recognition instruments, **1:338–340**
- DNA fingerprinting, **1:336–338**  
 genetic disease detection, 2:54  
 process of, 1:337–338
- DNA genome  
 structure of, 1:341  
 unique sequences, **1:340–342**
- DNA microarray technology, 2:56
- DNA science and technology, **1:335–336**  
 analysis aided by biosensor technology, 1:112  
 bacterial DNA, 1:80–81  
 biodetectors, 1:110–111  
 databases for identification, 1:73, 1:85  
 electrophoresis separation, 1:391  
 encoding secret messages, 1:341–342, 2:265, 2:279  
 implants into biological systems, 1:114–115  
 nanotechnology applications in, 2:295  
 profiling, 1:185  
 radiation damage to, 3:3  
 recombinant, 2:56, 2:406–407  
 sequences, **1:340–342**  
 viral genetics, 3:237–239  
 Watson-Crick model, 1:335
- DNFSB. See Defense Nuclear Facilities Safety Board (DNFSB), U.S.
- Document destruction, **1:342–344**, 1:343  
 burn box, 1:343
- Document forgery, **1:344–350**
- Document security  
 shredding, 1:343
- DOE. See Department of Energy (DOE)
- Doe, Sgt. Samuel K., 1:8
- Dogs  
 search and rescue at WTC, 2:15  
 sniffer, 1:164–165
- Dolphins (Marine Mammal Program), 2:249–251, 2:250
- Domestic Emergency Support Team (DEST), **1:356–357**
- Domestic intelligence, **1:357–358**
- Domestic Preparedness Office, U.S.  
 National (NDPO), **1:358**
- Domestic terrorist groups, 3:142–144
- Dominican Republic, U.S. intervention in, 1:29
- Donovan, William J., 1:199–200, 2:390, 3:208
- Doo transmitter, **1:359**
- Dosimeters, 1:359–360
- Dosimetry, **1:359–360**
- Double agents, **1:360–361**, 2:203  
 Aldrich H. Ames, 1:31–33  
 Aleksander Ogorodnik, 1:298  
 counterintelligence and, 1:275  
 George Blake, 1:102  
 Robert Philip Hansen, 1:316, 2:77–78
- Downey, John T., 2:207
- Doyle, Arthur Conan (1859–1930), 2:131  
 forensic geology usage in *A Study in Scarlet*, 2:33
- Drug Control Policy, U.S. Office of National, **1:362**
- Drug Enforcement Administration, U.S. (DEA), **1:312–315**, 1:313  
 interaction with FBI, 1:314  
 programs and goals, 1:315
- Drug-Free Communities Act (1997), 1:362
- Drugs and narcotics  
 barbiturates use as “truth serum,” 3:173  
 canine substance detection, 1:163–165  
 International Narcotics and Law Enforcement Affairs, U.S. Bureau of (INL), 2:139–140  
 socially acceptable during 1970’s, 1:313
- Drug trafficking  
 Bolivia, 1:133  
 narco-terrorism and, 1:281, 1:314
- Drug war, 1:30–31  
 anti-drug advertising, 1:362  
 DEA intelligence on, 1:314  
 Department of Defense lead agency for, 1:147  
 Reagan administration and, 1:313  
 Special Anti-narcotics Force (Bolivia), 1:133
- Drug war intelligence  
 National Drug Intelligence Estimate (NDIE), 1:363  
 NORAD tracking, 2:345
- DS&T. See Directorate of Science and Technology (DS&T, CIA)
- Dual use technology, **1:364–365**
- Duarte, Jose Napoleon, 1:29, 1:30
- Ducket, Carl, 2:452
- Dudayev, Pres. Dzhokhar (Chechnya), 1:172–173
- Dulles, Alan W., 1:195, 1:309–310  
 as Secretary of State, 1:325  
 Secret Intelligence Branch, 2:390
- Dzhoney, Nikolay Volodiev, 1:220
- Eastern Europe, Soviet communism in, 1:230–231
- East German intelligence agency (STASI), **3:114–115**, 3:115
- Ebola virus, **1:368–369**
- E-bombs, **1:369–370**, 1:384
- Echelon surveillance system, **1:370–372**  
 communication intercepts, 1:386  
 privacy rights and, 2:448
- Echosounders  
 use in bathymetric mapping, 1:95
- Economic espionage, **1:372–374**  
 Economic Espionage Act (1996), 1:190, 1:372, 1:374  
 MI6 and, 2:262  
 U.S. industry effects of, 1:373  
 vulnerabilities of, 1:372–373
- Economic intelligence, **1:374–376**  
 foreign, 1:375  
 Office of Research Reports (ORR), 1:374  
 resources, 1:375–376
- Economic interests and controls  
 for Chad oil revenues, 1:9  
 Marshall Plan (1947), 1:232, 1:233  
 Soviet Molotov Plan, 1:232
- Economy, U.S.  
 maintaining stability, 2:13–14  
 open market operations, 2:13
- Edmonds, Emma, 1:210, 1:212
- Egypt  
 espionage in ancient, 1:416  
 intelligence and security, **1:376**  
 London embassy bugged during Suez crisis, 1:404–405  
 looting of historical artifacts, 1:46
- Egyptian Islamic Jihad, 1:25  
 Al-Qaeda and the World Islamic Front for Jihad, 1:26
- Eichmann, Adolf, **1:376–378**, 1:377
- Einstein, Albert, 1:399, 2:22, 2:246, 2:295, 2:374
- Eisenhower administration (1953–1961)  
 China and Korean War, 1:379  
 Cuba intervention, 1:29  
 Eisenhower Doctrine, 1:237  
 end of Korean war, 2:208–209  
 Middle East independence of nations doctrine, 2:273  
 National Security Council, 2:356  
 national security policy, **1:378–379**  
 New Look program, 1:235  
 plan to depose Fidel Castro, 1:96  
 Project GENETRIX, 1:93–94  
 Sen. McCarthy and, 1:235  
 Southeast Asian Treaty Organization (SEATO), 1:237, 1:379  
 Tachen Straits crisis and nuclear threat, 1:237
- Eisenhower-Rockefeller letter forgery, 1:347
- El Salvador, 1:29

**I E I**

E-2C Hawkeye aircraft, **1:367–368**, 1:367

- civil war in, 1:30  
intelligence and security, **1:379–380**
- Electromagnetic spectrum, **1:381–384**, 1:388–389  
imaging technology, 1:392–393  
military and security significance of, 1:383–384  
multi and hyperspectral imagery, 2:60
- Electromagnetic weapons  
biochemical effects, **1:384–385**  
electromagnetic pulse (EMP), **1:380–381**
- Electronic communication intercepts  
Echelon, 1:370–372  
legal issues, **1:385–387**
- Electronic Communication Privacy Act (1986), 1:146  
computer crimes, 1:256
- Electronic Communications Privacy Act (1994), 2:146
- Electronic countermeasures, **1:387–388**
- Electronic data destruction, **1:255**
- Electronic devices  
limits of conventional, 2:461  
screening for, 1:22
- Electronic intelligence (ELINT)  
by aerial reconnaissance, 1:75  
Echelon, 1:370–372  
HUMINT vs., 1:385  
P-3 Orion aircraft modified for, 2:393  
ships designed for, 3:76–77  
TEMPEST technology, 1:385
- Electronic locks and keys, 2:236
- Electronics intelligence (ELINT)
- Electronic voice alteration, **3:242**
- Electronic warfare, **1:388–390**  
countermeasures to, 1:387–388  
e-bombs, 1:389–390  
electromagnetic pulse, 1:369–370
- Electron microscopy, 2:271
- Electro-optical intelligence, **1:390**
- Electrophoresis, **1:391–392**
- ELINT. *See* Electronic intelligence (ELINT)
- Ely, Eugene, 1:19
- Emergency planning  
Continuity of Government program (COG), 1:269–270  
Crisis Relocation Facilities, 1:269  
DOE Emergency Operations office, 1:355  
emergency response drill, 1:354  
EPA training and environment monitoring, 1:411  
military-civil training center, 2:303–304  
National Response System, 1:394  
Radiological Emergency Response Plan, 3:8
- Emergency Planning and Community Right-to-Know Act (EPCRA), 1:178, 3:200
- Emergency Response Teams, **1:393–395**, 1:394
- Emergency Response Technology Program (ERT), 3:136–137
- Emergency services  
Domestic Emergency Support Team (DEST), 1:356–357
- EM wave scanners, **1:392–393**
- Encryption standards  
Advanced Encryption Standard, 1:227, 1:228, 1:291, 1:396  
Data Encryption Standard, 1:207, 1:289, 1:291, 1:396  
Digital Encryption Standard, 1:227  
Escrowed Encryption Standard (EES), 1:218  
GSM mobile phone, 2:73–74
- Encryption systems and devices, 1:131–133, 1:286, 1:319–320  
algorithms, 1:396, 2:73  
of data, **1:395–396**
- Energy Department (DOE), United States. *See* Department of Energy (DOE)
- Energy directed weapons, **1:399–400**
- Energy harvesting, 3:26–27
- Energy policy  
energy crisis (1973–1974), 2:384  
energy technologies, **1:401–403**  
OPEC, 2:315, 2:384–385  
security issues, 1:402, 2:314–315
- Energy Regulatory Commission, U.S. Federal (FERC), **1:401**
- Energy Reorganization Act (1974), 1:354, 2:370
- Engelmann, Rudy J., 1:68
- Engineered Tissue Constructs (ETC), **1:111–112**
- Engines, scramjet, 2:91–92
- Engraving and Printing, U.S. Bureau (BEP), **1:403–404**
- ENIAC machine, 1:243
- Enigma cipher machine (WW II Germany), 1:131–132, 1:205, 1:206, 1:291, **1:405–407**, 1:406  
bombe development for deciphering, 1:131, 1:137, 1:206  
scrambler, 1:406–407  
U.K.—U.S. sharing of information on, 3:106
- Enterprise* (aircraft carrier), 1:19
- Entertainment industry, simulations for defense industry, 1:259–260
- Entry-Exit Registration System, U.S. National Security, **1:408**
- Environmental Measurements Laboratory, **1:409–410**
- Environmental policy  
Environmental issues impact on security, **1:408–409**  
EPA programs, **1:410–411**  
national security effects on, 1:409
- EPA (Environmental Protection Agency)  
Emergency Response Teams, 1:393–395
- National Response Team, 2:306–307
- EPCRA. *See* Emergency Planning and Community Right-to-Know Act (EPCRA)
- Epidemiological Intelligence Service, 1:168
- Epidemiology, **1:411–413**
- ERT. *See* Emergency Response Technology Program (ERT)
- Espionage, **1:413–414**  
Cambridge University Spy Ring, 1:151–155  
Chinese in U.S., 1:190–191, 2:133  
computer keystroke recorder, 1:258–259  
corporate, 1:255–256  
covert operations, 1:276–279  
Cuban operations against U.S., 1:292–293, 1:414  
early U.S., 3:22  
economic, 1:190, 1:342, 1:372–374  
in the Middle Ages, 1:417–418  
surveillance cameras in, 1:156–157
- Espionage Act (1917), **1:415**  
Socialist Party (U.S.), 2:122
- Espionage and intelligence  
historical foundations, **1:415–420**  
Soviet and Russian moles, 2:280–281
- Espionage technology and tools  
cameras and microfilm, 2:267–268  
drops, **1:361**  
impact of industrialization, 1:419  
KGB, 2:202–203  
tracedraft, 3:167  
World War I, 1:2
- Estonia, intelligence and security, **1:420**
- ETA. *See* Basque Fatherland and Liberty (ETA)
- Ethiopia, 1:7–8
- Ethnic profiling  
in screening process, 1:22
- Eukadi Ta Askatasuna. *See* Basque Fatherland and Liberty (ETA)
- European colonies (African), 1:6
- European Union, **1:420–422**
- European Union agencies, 1:422
- Evers, Medger, 2:8
- Executive orders and Presidential directives, **1:422–423**, 2:309
- Expendable launch vehicles, 2:298–299
- Explosive coal, **1:423–424**
- Explosives Unit (FBI)  
bomb damage assessment, 1:134
- Extraterrestrial Highway, 1:52
- Extraterrestrial life and UFO's, 1:51



F-22 Raptor, 1:388

F-117A Stealth Fighter, **2:1**, 2:2, 3:116

F/A-18 Hornet, 1:18, 1:400

- FAA (Federal Aviation Administration, U. S.), **2:2–3**  
 data parameter requirements for FDRs, 2:26  
 emergency responses to 9/11, 3:70  
 Facility security, **2:4–5**  
 Fair Credit Reporting Act (FCRA), 2:448  
 Fair Employment Practices Commission (FEPC), 2:7  
 Fatah Revolutionary Council. *See* Abu Nidal Organization (ANO)  
 FATF. *See* Financial Action Task Force (FATF)  
 Faulds, Henry (fingerprint identification), 2:17  
 FBI Explosives Unit  
     bomb damage assessment, 1:134  
 FBI (Federal Bureau of Investigation, U. S.), 1:13, **2:5–9**  
     assistance following chemical attacks, 1:179  
     COINTELPRO operations, 1:229–230, 2:8  
     computer keystroke recorder, 1:258–259  
     forensic use of DNA, 2:9  
     interaction with DEA, 1:314  
     PENTTBOM (9/11) investigation, 3:71  
     response to spy ring defections, 1:154  
     Un-American Activities Committee, U.S. House (HUAC), 2:253  
     United States v. Scarfo, 1:258–259  
 FBI (Federal Bureau of Investigation, U. S.) administration  
     careers in, 2:120–121  
     computer systems security measures, 2:8  
     counter-terrorism focus, 2:220–221  
     Freedom of Information Act requirements, 2:27, 2:28  
     history of, 2:6–8  
 FCC ( U.S. Federal Communications Commission), **2:9–10**  
     FM transmitter regulations, 2:26–27  
     National Telecommunications Information Administration, U.S. (NTIA), 2:312  
     radio frequency regulations, 3:5  
 FCRA. *See* Fair Credit Reporting Act (FCRA)  
 FDA (U.S. Food and Drug Administration), **2:10–11**  
     branch of HHS, 2:81  
     Public Health Service and, 2:455  
 Federal air marshals (FAM), 1:14–16, 1:15  
 Federal Aviation Act (1958), 2:2  
 Federal Emergency Management Agency (FEMA), **2:14–16**  
     assistance following chemical attacks, 1:179  
     Coast Guard National Response Center, 1:223  
     Crisis Relocation Facilities, 1:269  
     Mount Weather, 2:285–286  
     Radiological Emergency Response Plan, 3:8  
     World Trade Center activities, 1:50, 2:15  
 Federal Firearms Act (1938), 1:68  
 Federal language schools and tests, 2:216  
 Federal Open Market Committee, 2:13, 2:14  
 Federal Property and Administrative Services Act (1949), 2:11, 2:51  
 Federal Protective Service, U.S., **2:11–12**  
 Federal Railroad Administration (FRA)  
     Coast Guard National Response Center, 1:223  
 Federal Republic of Germany (FRG), 1:103  
 Federal Reserve Act (1913), 2:12  
 Federal Reserve System, U.S., **2:12–14**  
     banks in, 2:14  
 Federal Wiretapping Act (1968), 2:448, 3:138  
 FEMA. *See* Federal Emergency Management Agency (FEMA)  
 FEPC. *See* Fair Employment Practices Commission (FEPC)  
 FERC. *See* Energy Regulatory Commission, U.S. Federal (FERC)  
 Fermi, Enrico, 2:23, 2:247  
 FEST. *See* Foreign Emergency Support Team, U.S. (FEST)  
 Fe Ye, 1:373  
 Feynman, Richard, 2:246  
 Fibonacci, Leonardo (13th century mathematician), 1:288  
 Fighting Islamic Group, 1:25  
 Financial Action Task Force (FATF), 3:155, 3:157, 3:158  
 Financial intelligence  
     counterintelligence efforts, 1:73  
 Fincher, David (film director), 1:259  
 Fingerprinting analysis, **2:17–19**  
 Fingerprinting identification systems, 2:18, 2:19, 2:95  
 Finland, intelligence and security, **2:19–20**  
 First of October Anti-Facist Resistance Group (GRAPO), **2:20**  
 FISH (Geheimschreiber cipher machine). *See* Geheimschreiber cipher machine (WWII Germany)  
 Fission. *See* Nuclear fission  
 Flame analysis, **2:24–25**  
 Fleischmann, Martin, 2:45  
 Fleming, Ian, 2:132  
     Bond movies, 2:287–288  
 Flight crews (aircraft carriers), 1:18  
 Flight data acquisition unit (FDAU), 2:26  
 Flight data recorders, 2:25, **2:25–26**  
     data parameters recorded, 2:26  
 Flowers, Tommy, 1:242, 3:184  
 FM transmitters, **2:26–27**  
 FOIA. *See* Freedom of Information Act (FOIA, 1967)  
 Food supplies  
     Food and Cosmetic Act (1938), 2:10  
     Food and Drugs Act (1906), 2:10  
     Food contamination, 3:310  
     protection from bioterrorism, 2:29  
 Ford administration (1974–1977)  
     CIA restrictions, 1:194, 1:203  
     loss of S. Vietnam to communists, 2:30  
     National Security Council, 2:357  
     national security policy, **2:30**  
 Foreign Assets Control, U.S. Office (OFAC), **2:31**  
 Foreign Broadcast Information Service (FBIS), **1:198–199**  
 Foreign economic intelligence, 1:375  
 Foreign Emergency Support Team, U.S. (FEST), **2:16–17**  
 Foreign Funds Control (1940), 3:171  
 Foreign Intelligence Advisory Board, 1:194, 1:203  
 Foreign Intelligence Surveillance Act, **2:31–32**, 2:133, 2:448  
 Foreign Intelligence Surveillance Court of Review, **2:32–33**  
 Foreign technology intelligence  
     assisted strategic arms treaties, 1:76  
     U.S. economic espionage in, 1:373  
 Forensic chemistry, 1:183  
     chemical traces, 2:37  
     DNA fingerprinting, 1:338  
     solid-phase micro extraction techniques, 3:89  
 Forensic geology  
     in criminal investigations, 2:34–35  
     in military or intelligence operations, **2:33–35**  
 Forensic science, **2:36–39**  
     analytical methods, 2:38–39  
     bomb damage, 1:134  
     chemical applications in, 1:183–185  
     DNA fingerprinting in, 1:337  
     evidence and examination, 2:36–38  
     FBI's use of, 2:6–7  
     geology, 2:33–35  
     nuclear magnetic resonance, 2:373  
     nuclear spectroscopy, 2:372–373  
     polymerase chain reaction (PCR), 1:117, 2:38, 2:56, 2:433–436  
     seismology, 2:35  
     toxicology, 3:165  
 Forensic voice and tape analysis, **2:39–40**  
*Forrestal* (aircraft carrier), 1:19  
 Fouché, Joseph, 2:296–297  
 FRA. *See* Federal Railroad Administration (FRA)  
 France  
     aircraft carrier development, 1:19–20  
     balloon flight development, 1:91–92, 1:93  
     counter-terrorism policy, **2:40–41**  
     espionage in 19th century Great Britain, 2:297–298  
     French underground during World War II, 2:42–43  
     intelligence and security, **2:41–42**

- U.S.—Iraq anti-war position, 2:165  
 withdrawal from Vietnam, 3:232
- Franco-Prussian War, 1:2
- Franklin, Benjamin, 1:91  
 first postmaster general, 2:442
- Franks, Tommy R., 2:170
- Freedom of Information Act (FOIA, 1967),  
**2:27–28**
- Freedom of Information-Privacy Acts  
 (FOIPA), 2:28, 2:447–448
- French underground (World War II)  
 communications and codes, **2:42–43**  
 Jedburghs working with, 2:390
- Friedman, William, 2:460
- Fuel cells  
 research in hydrogen, 1:354, 1:402
- Fulbright, J. William, 2:189
- Fusion. *See* Nuclear fusion
- ## I G I
- G-2, **2:47**
- Galton, Sir Francis (fingerprint identifica-  
 tion), 2:17
- Gamma rays  
 role in EMP weapons, 1:383
- Gamow, George, 2:52
- GAO (General Accounting Office, U.S.),  
**2:48**
- Gas chromatography-Mass spectrometer,  
 1:175, 2:38–39, **2:49–50**, 2:50
- Gates, Robert, 1:148, 1:196, 1:311  
 Clinton intelligence briefing, 2:429
- Gaulle, Charles de, 2:43  
 French involvement in Vietnam,  
 3:232
- Geheimschreiber cipher machine (WWII  
 Germany), 1:205–206, **2:21**
- Geller, Uri (psychic), 2:453
- General Services Administration, U.S.  
 (GSA), **2:51**
- Genetic code, **2:52–54**, 2:53
- Genetic engineering  
 DNA implants, 1:114–115  
 identifying and detecting biological  
 weapons, 1:118, 2:278–279  
 recombinant DNA, 2:278  
 of vaccines, 3:86  
*See also* DNA science and  
 technology
- Genetics  
 Austrian database for identification,  
 1:73  
 bacterial, 1:82–84  
 disease detection and treatment,  
 2:54, 2:57  
 epidemiology, 1:412  
 ethics, privacy and security issues,  
**2:54–55**  
 technology of, **2:56–57**  
 testing, 2:53, 2:55  
 viral, 3:237–239
- See also* DNA detection and iden-  
 tification; DNA science and  
 technology
- Geneva conventions, 2:124–125
- Geneva Protocol (1925)  
 diplomatic control of biological  
 weapons, 1:116
- Genomics, **2:57–58**  
 applications of, 2:57–58  
 sequencing of pathogens, 2:404  
 of viruses, 3:237–238
- Geographic Information Systems (GIS),  
**2:64–65**, 2:248  
 crisis management and, 2:221–222  
 LIDAR system and, 2:234–235
- Geological Survey, U.S. (USGS), 2:425
- Geology  
 forensic, 2:33–35  
 military use of terrain intelligence,  
**2:58–59**  
 radar mapping and remote sensing,  
 2:59
- Geospatial imagery, **2:59–60**
- German-Bolshevik conspiracy forgery,  
 1:345–346
- German Democratic Republic (GDR),  
 1:103
- Germany  
 aerial reconnaissance, 1:74  
 Berlin Wall divides country, 1:103  
 counter-terrorism policy, **2:61**  
 cryptography, 1:3–4, 1:131–132,  
 1:291  
 East Berlin borders closed,  
 1:105–106  
 intelligence agencies, 1:2–3  
 intelligence and security, **2:62–63**  
 V-2 missile, 1:87, 1:89  
 WWI sabotage and intelligence op-  
 erations, 1:129–130  
*See also* Nazi Germany
- Gestapo, 1:3, **2:63–64**
- Ghauri (Pakistan), 1:88
- GIA. *See* Armed Islamic Group (GIA)
- Gibson, Steve, 1:262
- Gibson, William, 1:264
- GIS (Geographic Information Systems),  
**2:64–65**, 2:248  
 crisis management and, 2:221–222  
 LIDAR system and, 2:234–235
- Giuliani, Rudolph, 1:314
- Global Communications, U.S. Office  
 (OGC), **2:66**
- Global Expertise Reserve Program  
 (GERP), 2:326
- Global Positioning System (GPS).  
*See* GPS
- Global Protection Against Limited Strikes  
 (GPALS), 3:124
- Global Seismograph Network, 3:64
- Glomar Explorer*, **2:66–67**
- Goldwater-Nichols Department of  
 Defense Reorganization Act (1986),  
 2:190
- Goleniewski, Michael, 2:281
- Gorbachev, Mikhail (Soviet Premier),  
 2:202  
 announces nuclear testing morato-  
 rium, 1:254  
 Glasnost or “openness” and anti-  
 Communist movements, 1:241  
 Soviet economy and reforms,  
 1:240–241
- Göring, Herman, 2:63
- Gorshkov* (aircraft carrier), 1:20
- Gottlieb, Sidney (1918–), 1:108
- Government buildings  
 Federal Protective Service security  
 of, 2:11–12  
 GSA approved designs, 1:50, 2:51  
 Oklahoma City Federal Campus,  
 1:49  
 Ronald Reagan building, 1:49  
 security of, 1:50, 2:136–137
- Government Ethics, U.S. Office (OGE),  
**2:68**
- Government information  
 classification procedures, 1:213  
 Classified National Security Informa-  
 tion Act, 1:214–215  
 Freedom of Information Act, 2:27–28  
*See also* Classified information
- Government officials  
 protection of, 1:269–270  
 Shadow Cabinet, 1:269
- GPS (Global Positioning System),  
**2:68–70**, 2:69, 2:70  
 LIDAR system and, 2:234–235  
 mapping accuracy, 2:248
- GRAPO. *See* First of October Anti-facist  
 Resistance Group (GRAPO)
- Graves, Harold N. (FBI director), 1:198
- Great Depression, crime rates, 2:6
- Great Game, **2:70–72**
- Great Game Anglo-Russian Convention  
 (St. Petersburg, 1907), 2:72
- Greece  
 espionage in ancient, 1:416  
 intelligence and security, **2:73**  
 repatriation of Elgin Marbles, 1:46  
 Soviet incursions in, 1:233
- Greenspan, Alan (Federal Reserve chair-  
 man), 2:13
- Grenada  
 Operation Urgent Fury, 1:29  
 U.S. invasion of, 3:10
- Groves, Brig. Gen. Leslie, 2:246
- Gruinard Island, 3:109
- GSA, 1:49  
 government building approved de-  
 signs, 1:50
- GSM Encryption, **2:73–74**
- Guatemala, intelligence and security, **2:74**
- Guerrilla warfare, **2:74–75**
- Gun control legislation, 2:195  
 Federal Firearms Act (1938), 1:68  
 Gun Control Act (1968), 1:68  
 National Firearms Act (1934), 1:68



Organized Crime Act (1970), 1:68  
 Guns  
   ballistic fingerprints of, **1:85**  
   concealment techniques, 1:65  
   plastic bullets, 2:231  
   poison firing devices, 1:63–64, 1:65  
   residue analysis of, 1:184  
   revolvers, 1:63  
   silencers, **3:80–82**  
   submachine, 1:59  
   Taser, 3:134–135  
 Guzman, Abimael, 1:31

## I H I

Habash, George, 2:436  
 Habeas Corpus Act (1863), 2:121–122  
 Habyarimana, Maj. Gen. Juvenal, 1:7  
 Hackers. *See* Computer hackers  
 Hagalin, Boris (Swedish inventor), 1:206  
 Hager, Nicky, 1:372  
 Hague conferences, 2:124–125  
 Hahn, Otto (scientist, 1859–1968), 2:22, 2:375  
 Haig, Alexander, 2:358, 3:9  
 Haiti  
   intervention in, 1:30  
 Hale, Nathan, 1:417, 3:21  
 Hall, Reginald, 3:28  
 Halverson, Lt. Gail, 1:100  
 HAMAS (Islamic Resistance Movement), **2:77**  
 Hamilton, Alexander, 1:66, 3:169  
 Hansen, Robert, espionage case, 1:316, 1:361, **2:77–78**, 2:280–281  
 Harakat ul-Jihad Islami/ Bangladesh (HUJI-B) (Movement of Islamic Holy War), **2:79**  
 Harakat ul-Jihad Islami (HUJI) (Movement of Islamic Holy War), **2:78–79**  
 Harakat ul-Mujahidin (HUM) (Movement Holy Warriors), **2:79–80**  
 Hardening (computer systems), **2:80**  
 Harrier Jet, 1:20  
 Hassan-i-Sabah, Ismaili (1090 AD), 1:60  
 Hastart, U.S. Rep. Dennis, 1:214  
 Havel, Czech Pres. Vaclav, 1:303  
 Hayden, Michael, 2:352  
 Hazardous waste disposal  
   byproducts and waste, 2:369–370, 2:371, 2:381  
   PNNL research in, 2:394  
   Sandia Lab research in, 3:38  
 Health and Human Services Dep’t, U.S., **2:81**  
 Healthcare Research and Quality, Agency for (AHRQ), 2:455  
 Health Resources and Services Administration (HRSA), 2:455  
 Heavy water technology for nuclear development, **2:81–83**, 2:82–83, 2:247  
 Hebern, Edward, 1:291  
 Hegel, Georg W.F. (1771–1830), 3:148

Heinzen, Karl (1809–1880), 3:150  
 Heisenberg, Werner, 2:295  
 Helgerson, John L.  
   Clinton intelligence briefing, 2:429  
 Hellings, Martin, 3:102  
 Helms, Richard McGarrath, 1:196, 1:310  
 Helvey, Ephraim, 2:283  
 Hemlock  
   as a biochemical weapon, 1:106  
 Hemorrhagic fevers and diseases, **2:83–84**  
 Henry, Sir Edward (fingerprint classification), 2:17  
 Herzegovina. *See* Bosnia and Herzegovina  
 Heydrich, Reinhard, 1:2, 2:63  
 Hezbollah, 2:204  
 High-altitude Electromagnetic pulse (HEMP), 1:380–381  
 High power microwave weaponry, 1:399, **2:271–272**  
 Hillenkoetter, Rear Admiral Roscoe H., 1:195, 1:309  
 Himmler, Heinrich, 1:3, 2:63, 2:64  
 Hindenburg airship crash, 1:93  
 Hinkley, Jr., John  
   gun used in assassination attempt, 1:63  
 Hiroshima, Japan, 1:231, 2:23, 2:246  
 Hiss, Alger, 2:252  
 Hitchcock, Alfred (spy movies), 2:286  
 Hitler, Adolph (1889–1945), 2:63, 3:276, 3:278  
 Hizballa (Party of God), **2:84–85**  
 Ho Chi Minh (N. Vietnam leader), 3:232  
 Hollywood blacklist, 2:252  
 Holocaust  
   first intelligence on, 1:133  
   “Great Theft” of artwork, 1:47  
 Homeland Security, U.S. Dept. of, **2:85–88**  
   airline security, 1:22, 1:44–45  
   framework and directorates of, 2:87–88  
   Tom Ridge and, 1:124, 2:86  
   U.S. Coast Guard, 1:221, 2:87  
 Homeland Security Act, 2:86  
 Homeland Security Advisory System (HSAS), 3:140–142  
 Homing devices  
   doo transmitter, 1:359  
 Honecker, Ulbrecht Erich (Berlin Wall builder), 1:105  
 Hooke, Robert, 2:270  
 Hoover, J. Edgar (FBI director), 2:6  
   Un-American Activities Committee, U.S. House (HUAC), 2:253  
 Horsley, J. Stephen, 3:173  
 Houseman, John, 3:244  
 HUAC. *See* Un-American Activities Committee, U.S. House (HUAC)  
 Huang, John, 1:190  
 Hubble Space Telescope, 3:97  
 Hughes, Howard, 2:66–67

Hughes Electronic Corporation  
   Chinese rocket information exchange, 3:42  
 Hughes-Ryan Act (1974), 2:135  
 Human air plume, 1:16–17  
 Human decontamination, 1:316, 1:318–19  
 Human Genome Project, 2:55  
   microorganism detection and identification, 2:265  
 HUMINT (Human Intelligence), 1:193, **2:89**  
   ELINT vs., 1:385  
   used during Spanish-American War, 3:102–103  
 Hungary, intelligence and security, **2:90**  
 Hussein, Saddam, 2:162, 2:414–416  
   assassination attempt on Bush (H.W.), 2:416  
   48-hour deadline, 2:166  
   regime toppled, 2:175–176  
   war against, 2:169–176  
   *See also* Iraq; Operation Iraqi Freedom  
 Hwei Chen Yang, 1:190  
 Hydrogen bomb, 2:375, 3:258  
   Truman asks for, 1:232  
 Hydrogen fuel cell research, 1:354, 1:402  
 HyperSoar hypersonic aircraft, 2:91  
 Hypersonic aircraft, **2:90–92**  
 Hyperspectral imagery, 2:60, 2:248

## III

IBIA. *See* International Biometric Industry Association (IBIA)  
 IBIS (Interagency Border Inspection System), 1:45, **2:93–94**, 3:72  
 IDENT (Automated Biometric Identification System), **2:95**  
 Identification Friend or Foe (IFF), **2:98**  
 Identification systems  
   Automated Biometric Identification System (IDENT), 2:95  
 Identity theft, 1:342, **2:96–97**  
   Identity theft affidavit, 2:97  
   Identity Theft and Assumption Deterrence Act (1998), 2:97  
   Identity Theft Data Clearinghouse, 2:97  
   Pickler, Nedra (reporter), 2:96  
 IFF (Identification Friend or Foe), **2:98**  
 IKONOS remote sensing satellite, 3:43  
 Image intensification, 2:327–328  
 Image processing  
   electromagnetic spectrum, 2:248  
   software, 3:13–14  
 Imagery intelligence, 1:11–13, 1:12, 1:193, **2:99–100**  
 IMF (International Monetary Fund), **2:98–99**  
 Immigration and Naturalization Services (INS), **2:113–114**

- Immigration and Naturalization Service Passenger Accelerated Service System (INSPASS), **2:115–116**, 2:439
- IMS. *See* International Monitoring System (IMS)
- India
  - aircraft carrier development, 1:19
  - intelligence and security, **2:100–101**
  - looting of historical artifacts, 1:46
- Indian Health Services (IHS), 2:455
- Indonesia, intelligence and security, **2:101–102**
- Industrial Security Program (ISP), 1:321–322
- Infectious diseases, 1:170
  - epidemiology tracking, 1:411–413
  - Federal quarantine legislation, 1:250
  - hemorrhagic viruses, 2:83–84
  - pathogen transmission, 2:404–405
  - SARS isolation and quarantine, 1:248–252
  - security threats, **2:102–105**, 2:103, 2:264–265
  - smallpox, 3:84–85
  - underdeveloped countries susceptible to, 2:104
  - zoonoses, 3:286–287
- Information security, **2:105–106**
  - anti-virus software and, 2:105
  - breaches of, 2:105
  - cryptography and, 2:105–106
  - Information Security, U.S. Office (OIS), 2:106
- Information Security, U.S. Office (OIS), **2:106**
- Information Sharing and Analysis Centers (ISACs), 1:301
- Information warfare, **2:107–110**
- Infrared detection devices, 2:110, **2:110–112**
  - cameras, 1:390, 2:111
  - military applications for, 2:111
  - motion sensors, 2:284–285
  - police and security applications, 2:111–112
- Infrared imagers
  - countermeasures for, 2:112
  - designs for, 2:111
- Infrared spectroscopy, 3:107
- Infra-red waves
  - night vision and, 1:382, 2:111
  - stealth technologies, 3:117
- Infrastructure
  - components of, 1:282
  - Critical Infrastructure Assurance Office (CIAO), 1:282–283
  - Infrastructure Protection Center, U.S. National (NIPC), 2:112–113
  - protection of, 1:283, 3:62
- Infrastructure Protection Center, U.S. National (NIPC), **2:112–113**
- Inman, Admiral Bobby R., 1:330
- INS (Immigration and Naturalization Services), **2:113–114**
- InSAR (Interferometric Synthetic Aperture Radar), 2:248, 3:14
- INSCOM (U.S. Army Intelligence and Security Command), **2:114–115**
- Insecticide research, 2:321–322
- INSPASS. *See* Immigration and Naturalization Service Passenger Accelerated Service System (INSPASS)
- Inspector General, Office of the (OIG), **2:116–117**
- Institute for Creative Technologies, 1:260
- Institute of Future Space Transport, 2:91
- Insurance industry, terrorism risk insurance, **3:151**
- Intelligence, **2:117**
  - briefings to presidential candidates, 2:429
  - careers in, 2:119–121
  - history of U.S., 3:206–209
- Intelligence agencies
  - aiding crime prevention, 1:280–281
  - early U.S., 3:21
- Intelligence agent, **2:117–118**
  - International law and, 2:125
  - types of agents, 2:118
- Intelligence and counter-espionage careers, **2:119–121**
- Intelligence and democracy
  - anti-communism hysteria, 2:122–123
  - civil rights and liberties, 2:121–122
  - COINTELPRO illegal operations discrediting groups, 1:229–230
  - individual privacy and investigation policy, 2:123–124
  - issues and conflicts, **2:121–124**
  - Patriot Act and, 1:386–387
- Intelligence and international law, **2:124–125**
- Intelligence and Research, U.S. Bureau of (INR), **2:127**
- Intelligence and Security Committee, U.K., 2:168
- Intelligence and Threat Analysis (ITA), 1:330
- Intelligence Authorization Acts, U.S. Congress, **2:128**
- Intelligence community, **2:128–130**
  - American and European communities (WW I), 3:270–271
  - changes during Spanish-American War, 3:103
  - defining and formation of, 2:128–129, 3:21–22
  - Intelligence Community Executive Committee (IC/EXCOM), 2:129–130
  - Joint House-Senate Intelligence Committee, 2:129
  - oversight of, 1:194, 2:130, 2:135–136
  - psychotropic drugs and, 2:454–455
  - reorganization under National Security Act, 2:307–308
  - restrictions on, 2:126
  - tradcrafft, 3:167
  - United States, 3:202–204
- U.S. President and, 2:444–445
- Intelligence Identities Protection Act (1982), 1:203
- Intelligence Information Act (annual), 2:136
- Intelligence literature, **2:130–132**
- Intelligence officer, **2:133**
- Intelligence Oversight Act (1980), 1:203
- Intelligence Policy and Review, U.S. Office of (OPIR), **2:133–134**
- Intelligence research
  - Bureau of Intelligence and Research (INR) U.S. State Dep't, 1:323–324
  - Intelligence and Threat Analysis (ITA), 1:330
  - National Intelligence Estimates (NIEs), 1:324
  - Office of Research Reports (ORR, CIA), 1:374
- Intelligence retrieval
  - dead drop spike, 1:315
  - dead letter box, 1:315–316
  - ships designed for collection and, 3:76–77
- Intelligence Services Act, U.K. (1994), 2:262
- Intelligence sources, 1:193, 1:199
  - in Civil War escaped slaves as, 1:211
  - computer keystroke recorder, 1:258–259
  - data mining and databases, 1:307–308
  - dumpster diving, 1:299–300, 1:342
- Intelligence Support, U.S. Office of, **2:134**
- Interagency Border Inspection System (IBIS), 1:45, **2:93–94**, 3:72
- Interagency Security Committee, U.S., **2:136–137**
- Intercontinental ballistic missiles (ICBMs), 2:374, 3:261
  - Minuteman ICBM (U.S.), 1:87, 1:90
  - NORAD tracking, 2:345
  - See also* Ballistic Missiles
- Internal Revenue Service (IRS), 1:68, **2:137–138**
  - Criminal Investigation division, 2:138
  - Restructuring and Reform Act (1998), 2:137
- International Atomic Energy Agency (IAEA), **2:138–139**
  - Chernobyl disaster efforts of, 2:139
  - Iranian nuclear programs, 2:160–161, 2:164
  - LANL programs used by, 2:240
  - limitations of, 2:138–139
  - North Korea restricting inspections of, 2:347–349
  - nuclear weapon trafficking reports, 3:32
  - tracking nuclear materials, 3:255–257
- International Biometric Industry Association (IBIA), 1:121

- International Border Interdiction Training, 1:297
- International Commission on Missing Persons, 2:37
- International crime
- International Narcotics and Law Enforcement Affairs, U.S. Bureau of (INL), 2:139
- International Fusion Program, 2:45–46
- International law
- blocking terrorist financing, 3:158–159
  - Geneva conventions, 2:124–125
  - Hague conferences, 2:125
  - intelligence and, 2:124–125
  - International Law Enforcement Academies (ILEAs), 2:139
- International Monetary Fund (IMF), 2:98–99
- International Monitoring System (IMS), 1:254
- International Narcotics and Law Enforcement Affairs, U.S. Bureau of (INL), 2:139–140
- international crime efforts, 2:139
  - publications of, 2:139
- International Space Station, 3:97
- Internet, 2:140–143
- anti-spam legislation, 2:144
  - ARPANet and Internet history, 2:141–142
  - chat rooms and email, 2:148
  - commercial networks on, 2:142
  - guerilla tactics on, 2:75
  - ISP client information and Patriot Act, 1:387
  - WWW browsers, 2:142
- Internet security threats
- cyber attack and security, 1:301
  - hacking and cyber-crimes, 1:300, 2:142–143
  - surveillance, 2:145–147
- Internet service providers (ISPs), 2:142
- Internet spam and fraud, 2:144
- Internet spider, 2:144–145
- Internet surveillance, 2:145–147
- Electronic Communications Privacy Act (1994), 2:146
- Internet technologies
- IP addresses, 2:142, 2:143
  - protocols, 1:305, 2:141
  - tracking tools, 2:147–148
  - wireless, 1:300
- Internet tracking and tracing, 2:147–148
- INTERPOL (International Criminal Police Organization), 2:148–149
- INTERPOL, U.S. National Central Bureau, 2:150
- Interrogation, 2:151, 2:151–152
- See also Torture techniques and technologies
- Invisible ink, 3:58
- Ionizing radiation, 2:244
- IRA. See Irish Republican Army (IRA)
- Iran
- American hostages in, 1:166, 2:158–160, 2:274
  - biological weapons in, 1:114
  - IAEA inspectors in, 2:161
  - nuclear programs in, 2:160–161
  - Shah of Iran and U.S., 2:273–274
- Iran-Contra affair, 1:30, 2:155–157, 2:274
- conspiracy trials, 1:214, 1:331
- Iranian hostage crisis, 2:158–160, 2:159, 2:274
- Iran intelligence and security, 2:157–158
- Iran-Iraq war, 2:275
- nerve gas use in, 2:322
- Iraq
- American intelligence on, 2:416
  - anthrax production, 1:36–37
  - biological weapons in, 1:5, 1:114, 1:115, 1:334
  - botulism toxin in, 1:139
  - chemical weapons in, 2:165
  - intelligence and security agencies in, 2:161–162
  - looting of national museum, 1:47
  - propaganda in, 1:334
  - weapons inspections in, 2:162–167
- Iraq wars, 2:169–176, 2:170
- prelude to, 2:162–167
  - aftermath, 2:167–168
  - civil demonstrations for peace, 2:165
  - communication centers bombing, 2:171
  - media coverage of, 2:175
  - psychological warfare in, 2:173–174
- Ireland, intelligence and security, 2:176–177
- Irish Republican Army (IRA), 2:177–178
- Iris scans, 3:16–17
- IRS. See Internal Revenue Service (IRS)
- IRS Restructuring and Reform Act (1998), 2:137
- ISACs. See Information Sharing and Analysis Centers (ISACs)
- Islamic Army of Aden (IAA), 2:178
- Islamic fundamentalism, 1:331
- in Middle East, 2:273–274
- Islamic Movement of Uzbekistan (IMU), 2:178–179
- Islamic Resistance Movement (HAMAS), 2:77
- Islamic Union. See Al-Ittihad al-Islami (AIAl)
- Isotopic analysis, 2:179–180
- Israel
- Arab-Israeli wars, 2:273
  - counter-terrorism policy, 2:180–181
  - intelligence and security, 2:181–183
  - Palestinian conflict and terrorism, 3:149
  - Pollard espionage case, 2:430–431
  - USS Liberty incident, 3:218–220
  - Yom Kippur War, 2:284
- ITA. See Intelligence and Threat Analysis (ITA)
- Italy, aircraft carrier development, 1:19–20
- Italy, intelligence and security, 2:183–184
- ## I J
- Jackson, Henry, 2:198
- Jackson Subcommittee
- Kennedy and NSC, 2:198
- Jaish-e-Mohammed (JEM) (Army of Mohammed), 2:185
- Janjalani, Abdurajak Abubakar, 1:1–2
- Janjalani, Khadaffy, 1:2
- Japan
- aircraft carrier development, 1:19
  - espionage of Pearl Harbor, 2:412
  - intelligence and security, 2:186
  - Manchuria takeover by, 2:411
  - Purple cipher machine, 2:459–460, 3:185
  - trade embargo on, 2:411–412
- Japanese-American internment camps, 2:7, 2:122
- Japanese Red Army, 2:186–187
- JDAM (Joint Direct Attack Munition), 2:187–188
- Jedburghs (WWII), 2:390
- Jeffereys, Dr. Alec, 2:435
- Jefferson, Thomas, 1:28
- cipher wheel development, 1:289
- Jemaah Islamiya (JII), 2:188
- Jenner, Edward, 3:85, 3:221, 3:227
- Jerusalem
- U.N. declared international city, 2:181
- Jihad Group, 1:25
- Johnson, Clarence L., 3:82
- Johnson administration (1963–1969)
- Dominican Republic intervention, 1:29
  - national security, 2:188–189
  - National Security Council, 2:356–357
  - Tonkin Gulf Resolution, 2:189, 3:233
  - Vietnam war, 1:237
- Johnston, Philip, 3:264
- Joint Chiefs of Staff, U.S., 2:190, 2:191
- Joint House-Senate Intelligence Committee, 2:129
- Joint Task Force on Intelligence and Law Enforcement, 2:127
- Jonze, Spike (film director), 1:260
- Jordan, intelligence and security, 2:191–192
- Joyce, William (Lord Haw-Haw), 2:238–239
- J-STARs (Joint Surveillance and Target Acquisition Radar System), 2:192–193
- Judge advocate general (JAG), 2:276
- Judiciary Act (1789), 2:193
- Justice Department, U.S., 2:193–195, 2:194
- crime rate trends, 2:194–195
  - history, 2:193

- intelligence agencies in, 3:204
- K**
- Kabila, Laurent, 1:7
- Kahane Chai (Kach), **2:197**
- Karzai, Pres. Hamid (Afghanistan), 1:60
- Keeler, Leonarde, 2:433
- Kelly, David, 2:168
- Kennan, George, 1:234
- Kennedy, John F., 1:29
- assassination, 3:57
- Bay of Pigs (Cuba), 1:96, 1:97–98, 1:293–295, 2:198
- Berlin Wall, 1:105
- Continuity of Government program (COG), 1:269–270
- Cuban Missile Crisis, 1:252, 1:292, 1:294, 2:198
- missile gap with Soviet Union, 1:237, 2:198
- Peace Corps, 2:198
- Kennedy, Philip (robotics scientist), 1:140
- Kennedy administration (1961–1963)
- containment of Soviet expansionism, 2:197
- Jackson Subcommittee and NSC, 2:198
- military force buildup, 2:199
- National Security Council, 2:356–357
- national security policy, **2:197–199**
- Kenya
- bombing of U.S. Embassy, 2:200, **2:200–201**
- Keyhole intelligence satellites, 1:187, 1:310, 2:60, 3:15
- Imagery intelligence (IMINT) source, 2:100, 2:248
- KGB (Soviet Union), **2:201–203**, 3:30–31
- Berlin Tunnel, 1:102
- crime prevention control, 1:280–281
- dirty tricks, 1:331
- forgery operations, 1:347–348
- SMERSH (KGB assassination team), 1:63–64, 2:202
- surveillance cameras in, 1:156–157
- tactics of, 2:202–203
- use of double agents, 2:203
- Khmer Rouge, 2:154
- Khobar Towers bombing incident, **2:204**, 2:205
- Khomeini, Ayatolla R., 2:159
- Khrushchev, Nikita (Soviet Premier), 1:293–295
- Berlin and Germany political issues, 1:105–106
- Berlin Tunnel, 1:102
- U-2 incident, 3:179
- KH satellite series, 1:187
- KH series cameras, 1:155–156
- Kilby, Jack (engineer), 2:266
- Kilpatrick speech forgery, 1:348
- King, Jr., Martin Luther, 2:8
- Kissinger, Henry, 1:238, 2:30, 2:309, 2:334
- National Security Council, 2:357
- as Secretary of State, 1:325
- Kitty Hawk* (aircraft carrier), 1:18, 1:19
- Klaproth, Martin Heinrich, 3:211
- Knives and edge weapons, 1:64, **2:205–206**, 2:206
- Koestler, Arthur, 1:3
- Korea, North, 3:43
- China, nuclear technology and, 1:189
- intelligence and security, **2:346**
- nuclear capability estimates, 2:348–349
- nuclear weapons programs, **2:346–350**
- Pueblo* hijacking incident, 2:456–458, 3:77
- restricting nuclear program inspections, 2:346–349
- Soviet communications with, 2:456
- Korea, South, 2:209
- intelligence and security, **3:93**
- Korean War, 1:234, **2:206–210**
- Army Security Agency (ASA, U.S.), 1:56
- China involved in, 1:379, 2:208
- Epidemiological Intelligence Service development, 1:168
- Soviet disinformation in, 1:332
- Kosovo, NATO intervention of, **2:210–211**
- Ku Klux Klan, 3:143
- Ku Klux Klan Act (1871), 2:122, 3:143
- Kumpulan Mujahidin Malaysia (KMM), **2:211–212**
- Kurdistan Workers' Party, **2:212**
- Kurtz, Michael J., 1:216
- Kuwait Oil fires, **2:212–214**, 2:213
- Kuznetsov* (aircraft carrier), 1:20
- L**
- Lake, Anthony (NSC), 1:217
- Land mines clearance programs, **3:190–192**, 3:191
- Land Remote Sensing Policy Act, 3:43
- LANDSAT satellite program, 1:187, 2:60, 2:425
- Langley* (aircraft carrier), 1:19
- Langmuir, Irving, 2:259
- Language education training and skills, **2:215–216**
- Laporte, Pierre (Canadian state minister), 1:160, 1:162
- Large Volume Radiation Detector, 1:144
- Larson, John A., 2:433
- Laser, **2:216–218**
- LIDAR, 2:217–218
- listening devices, **2:218**
- Laser guided weapons, 1:400, 2:1, 2:217
- Laser radar, 1:390
- Laser weapons, 1:399
- Lashkar-e-Tayyiba (LT) (Army of the Righteous), **2:218–219**
- Laskar Mujahidin, 3:152
- Latin America
- communism in, 1:238–239
- drug war and gangs in, 1:30–31
- IMF focus on, 2:99
- nationalism during Napoleonic wars, 2:281–282
- U.S. Army School of the Americas, 1:29
- U.S. security policy and interventions, 1:28–31
- Launch vehicles, expendable, 2:298–299
- Law enforcement
- Australia, 1:72
- ballistic fingerprints, 1:85
- CIA and, 1:281
- federal training centers, 2:222–224, 2:303–304
- International Narcotics and Law Enforcement Affairs, U.S. Bureau of (INL), 2:139–140
- providing intelligence to, 2:126
- psychotropic drugs and, 2:454–455
- responses to terrorism, 2:219–222
- surveillance systems, 1:220–221
- Law enforcement Partnership to Combat Terrorism Act (2002), 2:222
- Law Enforcement Training Center, U.S. Federal (FLETC), **2:222–224**, 2:223
- Lawrence, Ernest Orlando, 2:224
- Lawrence Berkeley National Laboratory (LBL), **2:224–225**
- Lawrence Livermore National Laboratory (LLNL), 2:44, **2:225–226**
- high power microwave weaponry, 2:272
- L-Gel decontaminant, 2:230–231
- nucleic acid analyzer, 2:379
- Lazar, Robert, 1:51
- League of Nations, **2:226–227**
- Lebanon, bombing of U.S. embassy and barracks, **2:227–228**
- Lebed, Alexander (Soviet diplomat), 1:173
- Lee, Gen. R. E., 1:211, 1:212
- Leeuwenhoek, Anton van (Dutch naturalist, 1660's), 1:80
- Left-wing terrorists, 3:144–145
- Lenin passport forgery, 1:345
- Less-lethal weapons technology, **2:229–230**, 2:230
- Leventhal, Todd, 1:334
- Lew, Elizabeth Van, 1:212
- Lexington* (aircraft carrier), 1:19
- L-Gel decontamination reagent, 1:317–318, **2:230–231**
- Liberation Tigers of Tamil Eelam (LITE), **2:231–232**
- Liberia, ethnic oppression in, 1:8
- Libicki, Martin C., 2:107
- Libraries and Information Sciences, U.S. National Commission on (NCLIS), **2:232**



- Libya  
intelligence and security, **2:233**  
PanAm 103 bombing and trial of  
Libyan agents, 2:398–400  
support of terrorist groups, 2:275  
U.S. attack of (1986), **2:233–234**
- Libyan Fighting Group, 1:25
- Libyan Islamic Fighting Group, 1:25
- LIDAR (Light detection and ranging),  
2:217–218, **2:234–235**, 3:14
- Life Support for Trauma and Transport  
(LSAT), 1:120
- Limited Test Ban Treaty, 1:253
- Listening devices, 1:145–147  
Electronic Communication Privacy  
Act (1986), 1:146  
noise generators, 2:341
- Litvinenko, Alexander, 2:131
- Lloyd, William Alvin, 3:206–207
- Lockheed Martin Aeronautics Company  
Skunk Works, 3:82–83
- Lockpicking, **2:235**
- Locks and keys, **2:236**
- Lombroso, Cesare, 2:433
- Lonetree, Clayton J., 3:74–76
- Long, Breckinridge (Dept. of State), 1:198
- Long, John, 1:164
- Long Duration Exposure Facility (LDEF),  
2:320
- Looking Glass (Airborne Command Post),  
**2:237**, 2:238
- “Loose nukes,” 3:32–33
- Loral Space and Communications Corp.,  
1:322, 3:42
- Lord Haw-Haw (William Joyce),  
**2:238–239**, 2:450
- Lord’s Resistance Army (LRA), **2:239**
- Los Alamos National Laboratory (LANL),  
**2:239–241**  
supercomputer at, 2:240  
Wen Ho Lee, 1:190, 1:191, 1:213,  
2:133
- Los Angeles International Airport, 1:21
- Los Angeles Olympics leaflet forgery,  
1:348
- Louvre Museum (France)  
protection of art and antiquities,  
1:46, 1:47
- Lowe, Thaddeus, 1:92
- Loyalist Volunteer Force (LVF), **2:241**
- LSAT. *See* Life Support for Trauma and  
Transport (LSAT)
- Lugar, Richard, 3:32
- Luminoso, Sendora, 1:31
- Lumumba, Patrice (Congo Prime Minis-  
ter), 1:7, 1:108, 1:237
- Luria, A.R., 2:433
- MacArthur, U.S. Gen. Douglas, 1:234  
Korean war, 2:208
- MacCracken, Jr. William P., 2:2
- MacDonald, Sir John A. (Canadian Prime  
Minister), 1:161
- Machiavelli, Niccolo, 1:418
- Maclean, Donald, 1:153
- MAD. *See* Mutually Assured Destruction  
(MAD)
- Mad man theory, Richard Nixon, 1:238
- Magaw, John, 3:104
- Magnetic resonance imaging (MRI), 1:141
- Mail sanitization, **2:243–245**, 2:442
- Malicious data, **2:245**
- Manchuria, Japanese takeover of, 2:411
- Mandela, Nelson, 1:8
- Maneuverable reentry vehicles (MARV),  
1:89–90
- Manhattan Project, 1:231, **2:245–247**,  
2:246, 2:375  
Oak Ridge National Laboratory  
(ORNL), 2:381  
security for, 2:247
- Mann Act (1910), 2:6
- Mao Tse Tung (Mao Zedong, Chinese  
leader), 1:233, 2:208
- Maps and mapping technology, **2:248**  
bathymetric, 1:95–96  
Geographic Information Systems  
(GIS), 2:64–65  
National Imagery and Mapping  
Agency (NIMA), 2:331
- Marine mammal program, **2:249–251**  
Marine Mammal Systems (MSS),  
2:251  
MSS deployments, 2:251
- Marines, U.S.  
National Maritime Intelligence Cen-  
ter, 2:336–337
- Marine traffic monitoring  
U.S. Coast Guard, 1:221–222
- Maritime Security Act (2002), 2:438–439
- Markov, Georgi, 1:63–64, 1:107
- Marshall, George (1880–1959), 1:232  
as Secretary of State, 1:325
- Marshall Plan (1947), 1:232, 1:233
- Marston, William M., 2:433
- Martial law  
Posse Comitatus Act (1878) and,  
2:126  
Reconstruction period (1865–1877),  
2:126
- Martin, Archer, 2:49
- Martin, Kate, 2:27
- Maskhadov, Pres. Aslan (Chechnya),  
1:173
- Mass spectrometry, 2:38
- Mathematical modeling  
software for, 1:259–260
- Matthei, Heinrich, 2:52
- Maugham, W. Somerset, 2:262
- Maxim, Hiram P., 3:80
- Mayaguez* (U.S. merchant ship)  
communist capture of, 2:30
- McCain, John S. (U.S. senator), 1:4
- McCarthy, Timothy J., 3:56
- McCarthy, U.S. Sen. Joseph, 1:233–234,  
1:235, 2:123, 2:207, **2:251–253**
- McClellan, Gen. G.B. (U.S. Civil War),  
1:211, 1:212
- McCone, John A., 1:195–196, 1:201,  
1:310, 3:208
- McFarlane, Robert C., 2:156
- McGonagle, Comm. William, 3:218
- McNamara, Robert S., 1:327, 2:189
- McVeigh, Timothy, 3:144
- Measures and Signatures Intelligence  
(MASINT), **2:253–254**
- Medical Research Institute of Chemi-  
cal Defense, U.S. Army (USAMRDC),  
**3:213–214**
- Medical Research Institute of Infectious  
Diseases, U.S. Army (USAMRIID),  
3:214, **3:214–216**
- Medical science resources  
Centers for Disease Control and  
Prevention (CDC), 1:168–170  
dual use technologies, 1:365  
Epidemiological Intelligence Service,  
1:168  
infectious diseases, 1:170  
LBL research in, 2:224
- Meeks, Elsie (Civil Rights Commission),  
1:247
- Meitner, Lise, 2:22
- Menzies, Stewart, 2:262
- Merer, RAF Air Comm. J.F., 1:100
- Metal detectors, **2:254–256**, 2:255
- Meteorology  
measuring instruments, 2:256  
satellites, 2:257  
weather alteration and, **2:256–260**
- Meusnier, Jean-Baptiste-Marie, 1:93
- Mexico  
intelligence and security, **2:260**  
Pancho Villa, 1:28
- M15 (British Security Service), **2:260–261**,  
3:194  
Cambridge University Spy Ring,  
2:261  
Suez crisis, 1:404–405  
work against German and Soviet  
infiltrators, 2:261
- M16 (British Secret Intelligence Service),  
**2:262**, 2:263, 3:195  
Bletchley Park cryptanalysis, 2:262
- Microbiology  
applications of, **2:263–266**  
genetic detection and identification,  
2:265
- Microchip, **2:266–267**
- Microdot cameras, 1:159–160
- Microelectronics, 2:461
- Microfilms, **2:267–268**, 2:268
- Microorganisms as biological weapons,  
2:264–265
- Microphones, 1:146, **2:268–270**, 2:269,  
3:78  
parabolic, 2:403  
types of, 2:268–269

- Microprocessors, 2:266  
     bio-flip implants, 1:112  
     Moore's Law, 2:266–267
- Microscopes, **2:270–271**
- Microwave weaponry  
     high power, **2:271–272**
- Middle East  
     anti-American sentiment in, 2:66  
     espionage in ancient, 1:416  
     independence of nations, 2:273  
     Islamic fundamentalism, 2:273–274  
     rise of terrorism in, 2:272–273  
     Soviet incursions in, 1:233  
     U.S. defense against communism, 1:237  
     U.S. security policy and interventions, **2:272–275**
- Middle East oil  
     U.S. dependency on, 1:147, 1:166
- Midway, battle of, 1:19
- Military aircraft testing facility, 1:51
- Military intelligence  
     Germany, 1:74  
     Russia, 1:74  
     United States, 1:243–244, 1:327–329, 2:47  
     use of terrain intelligence, 2:58–59
- Military Joint Intelligence Center (NMJIC), United States, 1:327
- Military personnel  
     anthrax vaccine, 1:37, 1:39  
     Berlin Airlift operations, 1:100–101  
     Persian Gulf War arsenal, 2:415–416  
     Special Forces, 1:322
- Military police, U.S., **2:276**
- Milosevic, Slobodan, 2:210
- Ming Zhong, 1:373
- Miniature cameras, **1:157–160**  
     microdot camera, 1:159–160  
     Minox camera, 1:265–266, 2:267  
     pinhole camera, 1:158  
     Tokya 78-M (Soviet), 1:157  
     video camera, 1:158  
     wristwatch cameras, 1:159
- Mini-Ramen LIDAR System (MLRS), 1:143
- Minox camera, 1:158–159, 1:265–266, 2:267
- Minuteman ICBM (U.S.), 1:87, 1:90, 2:374
- MIRV (Multiple independently targetable reentry vehicle), 1:89, 1:90, 2:30
- Missile defense lasers, 2:217
- Missiles  
     categories of, 1:89  
     flight profile, 1:89–90  
     payloads and warheads, 1:90
- Mitnick, Kevin, 1:257
- MOAB (Massive Ordnance Air Burst Bomb), **2:276–278**, 2:277
- Mobilization Against Terrorism Act (MATA), 2:114
- Mobutu, Joseph Désiré, 1:6
- Mohammed, Khalid Sheikh, 1:49
- Molecular biology applications, **2:278–279**
- Moles, **2:279–281**
- Molotov Plan (Soviet Union), 1:232
- Monge, Gaspard (18th century mathematician), 1:259
- Monroe Doctrine, 1:28, **2:281–282**
- Montague, Lady Mary Wortley, 3:221, 3:227
- Montes, Ana B., 1:292
- Montgolfier, Jacques-Etienne (French balloon pilot), 1:92
- Montgolfier, Joseph-Michel (French balloon pilot), 1:92
- Moore, Gordon (engineer), 2:266–267
- Moore's Law (microchip electronics), 2:266–267
- Morgan, John Hunt (Confederate Cavalry), 1:211
- Morgenthau, Henry, 3:170–171
- Morocco, intelligence and security, **2:282–283**
- Moro National Liberation Front, 1:1–2
- Morse, Samuel F. B., 1:289, 1:419
- Morse code, 1:225, 1:289, 1:419
- Mossadegh, Mohammed (Iranian Premier), 1:195
- Mossad (Israeli Institute for Intelligence and Special Tasks), 2:283, **2:283–284**  
     resources and organization, 2:284  
     Wrath of God team response to Munich Olympics, 2:283–284  
     Yom Kippur War, 2:284
- Mössbauer spectroscopy, 3:108
- Most, Johann (1846–1906), 3:150
- Motion sensors, **2:284–285**
- Mountin, Dr. Joseph M. (CDC director), 1:168
- Mount Weather (COG safety site), **2:285–286**
- Movies  
     Alfred Hitchcock and spy, 2:286  
     “Dr. Strangelove,” 2:287  
     espionage and intelligence portrayals, **2:286–289**  
     ethnic portrayals in, 2:289  
     James Bond series, 2:287–288  
     terrorism in, 2:289
- Mozambique, 1:8
- MPLA. *See* Popular Movement for the Liberation of Angola (MPLA)
- Mujahedin-e-Khalq Organization (MEK or MKO), **2:290**
- Mullany, Pat, 2:449
- Mullis, Kary B., 2:433
- Multispectral imagery, 2:60, 2:248
- Munitions, unexploded ordnance clearance programs, 3:190–191
- Mussolini, Benito, 3:276
- Mustard gas, **2:290–291**, 2:291
- Mutually Assured Destruction (MAD), 1:42, 2:189
- Myers, Gen. Richard B., 1:306
- NI**  
     Nagasaki (Japan), 1:231, 2:23, 2:246  
     NAILS (National Automated Immigration Lookout System), **2:293**  
     Nanotechnology, **2:294–296**  
         applications in, 2:295–296  
         genetic studies, 2:56  
         National Nanotechnology Initiative, 2:296  
         quantum physics and, 2:294–295  
     Napoleonic wars  
         espionage during, **2:296–298**  
         Latin American nationalism during, 2:281–282  
     Narcotics. *See* Drugs and narcotics  
     NASA (National Aeronautics and Space Administration), **2:298–299**  
         airline security, 1:141  
         creation of, 1:237  
         DARPA programs transferred to, 1:306  
         hypersonic aircraft, 2:91  
         Mars Pathfinder mission, 3:26  
     Nassar, Pres. Gamel (Egyptian)  
         Baghdad Pact, 1:237  
         Soviet ties and Suez canal crisis, 1:404–405, 3:127  
     Nassr Engineering Manufacturing facility (Iraq), 1:351  
     National Advisory Committee for Aeronautics (NACA), 2:90  
     National Aeronautics and Space Administration. *See* NASA  
     National Airspace System (NAS), 2:3  
     National Archives Act (1934), 2:300  
     National Archives and Records Administration (NARA), **2:300**  
         declassified information received by, 1:216  
     National Center for the Analysis of Violent Crime (NCAVC), 2:448–449  
     National Command Authority, **2:300–301**  
     National Communications System, U.S., **1:252**  
     National Contingency Plan (NCP), 1:394  
     National Counterintelligence Policy Board, 1:324  
     National DNA Database (NDNAD), 1:85  
     National Drug Intelligence Estimate (NDIE, Canada), **1:363**  
     National Drug Threat Assessment, **2:301**  
     National Firearms Act (1934), 1:68  
     National Imagery and Mapping Agency (NIMA), 2:60, 2:248, **2:331**  
         declassified documents, 1:216  
         Photographic Interpretation Center (NPIC), 2:423  
     National Information Infrastructure Protection Act, U.S. (1995), **2:301–302**  
     National Institute of Justice (NIJ), **2:330**  
     National Institute of Mental Health (NIMH), **2:332**

- National Institute of Standards and Technology (NIST), 1:245, 1:246, **2:332–333**  
 Computer Security Division, 2:333–334
- National Institutes of Health (NIH), **2:329–330**, 2:455  
 BioShield Project, 1:123  
 protective measures development, 1:126
- National Integrated Ballistics Identification Network, 1:85
- National Intelligence Council, **2:325–326**
- National Intelligence Estimates (NIEs), 1:324, **2:302–303**, 2:325  
 criticism of, 2:303
- National Interagency Civil-Military Institute, U.S. (NICI), **2:303–304**
- National Liberation Army (ELN), **2:304**
- National Military Joint Intelligence Center, **2:305**
- National Missile Defense (NMD), 3:124–125
- National Money Laundering Strategy (NMLS), 3:156–157
- National Nanotechnology Initiative, 2:296
- National Nuclear Security Administration (NNSA), **2:337–340**
- National Oceanic and Atmospheric Administration (NOAA), **2:340–341**  
 Cospas- Sarsat satellite system, 2:341  
 National Weather Service, 2:340
- National Pharmaceutical Stockpile Program (NPS), 1:126, 1:319
- National Preparedness Strategy, U.S., **2:305–306**
- National Reconnaissance Office (NRO), **2:350–351**, 3:46
- National Response System, 1:394
- National Response Team, U.S., **2:306–307**
- National School of Biological Sciences (Mexico), 1:184
- National Science Foundation (NSF), 2:141–142, **2:360**
- National Security Act (1947), 1:193, 1:200, 1:202, **2:307–308**  
 Truman presenting to Congress, 1:234
- National Security Advisor, U.S., **2:308–310**, 2:354
- National Security Agency (NSA), **2:351–353**  
 careers in, 2:120  
 document declassification, 1:215–216  
 secrecy of, 2:351–252
- National security and emergency preparedness (NS/EP), 1:252
- National Security Council (NSC), 1:149, **2:353–355**, 2:354  
 Clinton administration, 1:217  
 Cold War operations, 1:232  
 history of, 1:200, **2:355–359**  
 Kennedy and Jackson Subcommittee, 2:198  
 memorandum 68, 1:234  
 republican administrations, 2:353–354  
 U.S. President and, 2:444–445
- National Security Strategy, U.S., **2:310–311**
- National Security Telecommunications Advisory Committee, **2:311**
- National Telecommunications Information Administration, U.S. (NTIA), **2:312**
- National Transportation Safety Board (NTSB), **2:360–362**
- National Union for the Total Independence of Angola (UNITA), 1:8
- National Weather Service, 2:257, 2:340
- NATO (North Atlantic Treaty Organization), **2:312–314**, 2:313  
 Berlin Wall, 1:103  
 deterrence strategies to biological warfare, 1:125–126  
 formation of, 1:232, 1:233  
 Kosovo intervention, 2:210–211
- Natural resources, national security, **2:314–315**
- Navaho Indians (Code-talkers), 1:291, 3:263–265
- Navigational satellite systems  
 GPS (Global Positioning System), 2:68–70  
 Navstar, 2:68
- Navigation tools, 2:68–69
- Navstar, 2:68
- Navy, U.S.  
 aircraft carrier development, 1:19  
 NMIC (National Maritime Intelligence Center), 2:336–337  
*Pueblo* incident and Project Clickbeetle, 2:456, 3:77  
 ships designed for intelligence collection, **3:76–77**
- Navy Criminal Investigation Service (NCIS), **2:316**
- Nazi Germany  
 art and antiquities “Great Theft,” 1:47  
 Gestapo and Abwehr, 1:3  
 Nazi Security Service, 1:2  
 propagandist for, 2:238–239  
 psychological warfare in, 2:108–109
- NCIX (National Counterintelligence Executive, U.S. Office of the), **2:317–318**
- NCLIS. *See* Libraries and Information Sciences, U.S. National Commission on (NCLIS)
- NDIC (National Drug Intelligence Center, Dep’t of Justice), 2:318, **2:318–319**
- NDNAD. *See* National DNA Database (NDNAD)
- Near-space environment, **2:319–321**  
 Long Duration Exposure Facility (LDEF), 2:320  
 nuclear devices in, 2:319–320
- Nebel, Fritz, 1:4
- Nechaev, Sergei (1847–1882), 3:150
- Nedrow, Roy D., 2:316
- Nellis Air Force Base (U.S.), 1:51
- Nerve gases, **2:321–322**, 2:322  
 G and V agents, 2:322  
 Soman, 3:89–90  
 Tabun, 2:321–322, 3:133  
 VX nerve agent, 3:246–247
- NEST. *See* Nuclear Emergency Support Team (NEST)
- Netherlands, intelligence and security, **2:323**
- New People’s Army (NPA), **2:323–324**
- Newsham, Margaret, 1:372
- News media, war coverage, 1:305
- New Zealand, intelligence and security, **2:324**
- NFIB (National Foreign Intelligence Board, U.S.), **2:325**
- Ngo Dinh Diem (S. Vietnam Prime Minister), 1:237, 3:232
- Nicaragua  
 Communists in, 1:196  
 Contras and Sandinistas in, 1:30  
 intelligence and security, **2:326–327**  
 occupation of, 1:28  
*See also* Iran-Contra affair
- Nichols, Terry, 3:144
- Nicolai, Walther, 1:2
- Nigeria  
 intelligence and security, **2:327**  
 police force and criminal activity in, 1:9
- Night vision scopes, **2:327–329**, 2:328  
 image intensification, 2:327–328  
 infrared imaging, 2:111–112, 2:328–329, 2:382
- NIH (National Institutes of Health), **2:329–330**, 2:455  
 BioShield Project, 1:123  
 protective measures development, 1:126
- Nimitz class aircraft carriers, 1:18, 1:19
- NIPC. *See* Infrastructure Protection Center, U.S. National (NIPC)
- Nirenberg, Marshall, 2:52
- NIST (National Institute of Standards and Technology), 1:245, 1:246, **2:332–333**  
 Computer Security Division, **2:333–334**
- Nixon, Richard M., 1:237–238  
 Chile intervention, 1:29  
 China visit, 1:238, 2:335  
 kitchen debate with Khrushchev (as V.P.), 1:235  
 redefining Cold War—Nixon Doctrine, 1:237–238  
 stopped biological weapons research, 1:116
- Nixon administration (1969–1974), **2:334–335**  
 National Security Council, 2:357  
 Security Council, 2:335  
 Vietnam withdrawal, 3:234

- Watergate scandal, 1:202, 2:335
- NMIC (National Maritime Intelligence Center), **2:336–337**
- Marine and Coast Guard components, 2:337
- Naval components of, 2:336
- Office of Naval Intelligence (ONI), 2:336–337
- NNSA (National Nuclear Security Administration), **2:337–340**
- NOAA. *See* National Oceanic and Atmospheric Administration (NOAA)
- Noble, Ronald (INTERPOL), 2: 149
- Noise generators, **2:341**
- Non-governmental global intelligence and security, **2:342–343**
- Nonproliferation and national security, U.S., **2:343**
- Non-Proliferation Treaty (NPT)
- North Korea and NPT Safeguards agreement, 2:349
- Nonproliferation Verification Research and Development Program (NNSA), 2:339
- NORAD (North American Air Defense Agreement), 2:344, **2:344–346**, 2:345
- drug smuggling and trafficking and, 2:345
- Noriega, Manuel (Panamanian dictator), 1:29, 1:30, 1:279, 1:310, 2:109
- North, Oliver, 2: 155, 2:156, 2:358
- North Atlantic Treaty Organization (NATO), **2:312–314**, 2:313
- Berlin Wall, 1:103
- deterrence strategies to biological warfare, 1:125–126
- formation of, 1:232, 1:233
- Kosovo intervention, 2:210–211
- North Korea. *See* Korea, North
- Northrop Grumman, B-2 Bomber, 1:79
- Norway, intelligence and security, **2:350**
- Norwood, Melita, 1:230
- Noyce, Robert (engineer), 2:266
- NPIC. *See* Photographic Interpretation Center, U.S. National (NPIC)
- NPS. *See* National Pharmaceutical Stockpile Program (NPS)
- NRO (National Reconnaissance Office), **2:350–351**
- NSA. *See* National Security Agency (NSA)
- NTA. *See* Anti-imperialist Territorial Nuclei (NTA, Italy)
- NTTC. *See* Technology Transfer Center, National (NTTC)
- Nuclear, biological, and chemical defense, Surgeon General and, **3:129–130**
- Nuclear arms control, 2:366
- dismantling, 1:321
- International Monitoring System (IMS), 1:254
- START I Treaty, **3:112–113**
- START II Treaty, 3: 113, **3:113–114**
- verification of, 1:254
- Nuclear Emergency Support Team (NEST), 2:239–240, 2:363, **2:363–364**, 2:364
- Nuclear Fission, **2:22–24**, 2:365–366
- Nuclear Fusion, **2:44–46**, 2:375
- as energy source, 2:45–46
- fusion sequence, 2:44–45
- Nuclear magnetic resonance, 3:108
- Nuclear materials
- byproducts and waste, 2:369–370, 2:371, 2:381
- decontamination, 1:318, 1:321
- safeguarding, 3:255–256, 3:257
- tracking methods, **3:256–257**
- Nuclear power plants, **2:365–368**
- aircraft carriers, 1:19
- Chernobyl, 1:68, 1:185–188
- dependent on heavy water development, 2:82–83
- first reactor for energy production, 2:23
- public perception of, 2:372
- security of, 2:365–368
- Three Mile Island, 1:68, 2:365, 2:372
- Nuclear proliferation, 2:365
- nonproliferation, 2:343, 2:377
- nuclear arms race, 1:166–167, 2:375
- Nuclear reactors, 2:23, 2:368, **2:368–370**
- naval, 2:370
- neutron moderation in, 2:82
- nuclear chain reactions, 2:246
- satellite mishaps with, 2:319–320
- Nuclear Regulatory Commission (NRC), **2:370–372**, 2:371
- Nuclear safety and security
- Argonne National Laboratory, 1:53
- dismantling, 1:321, 3:32
- DOE office of security, 1:353
- National Nuclear Security Administration, 2:337–340
- Nuclear Emergency Support Team, **2:363–364**
- radiation detectors, **2:362–363**
- threat assessment, 2:339, 2:367, 3:32–33
- Nuclear spectroscopy, **2:372–373**
- Nuclear testing
- Comprehensive Test Ban Treaty (CTBT), 1:253–254
- Limited Test Ban Treaty, 1:253
- Threshold Test Ban Treaty, 1:253–254
- U.S. and Russia announces testing moratorium, 1:254
- Nuclear warfare, nuclear winter theory, 2:376–377, **2:378–379**
- Nuclear weapons, **2:374–378**
- biological damage from, 3:3–4
- certification and testing of, 2:225–226
- declassified information mistake, 1:191
- LLNL research in, 2:225–226
- “loose nukes,” 3:32–33
- Manhattan Project, 2:245–247
- radiation detectors, 2:362–363
- Russian security of, 3:31–33
- smuggling of, 2:339
- types and sizes of, 2:377
- Nucleic acid analyzer, **2:379–380**
- Number theory, cryptography and, 1:286–287
- Nunn, Sam, 3:32
- Nunn-Lugar Threat Reduction Program, 3:32
- Nye, Jr., Joseph S., 2:303

## I O I

- Oak Ridge National Laboratory (ORNL), **2:381–382**, 2:382
- chemical-biological mass spectrometer (CBMS), 2:179, 2:381
- Ocean mapping. *See* Bathymetric maps
- Office of Naval Intelligence (ONI), 2:336–337
- Office of Research Reports (ORR, CIA), 1:374
- Office of Strategic Services (OSS), U.S., 1:199–200, **2:389–391**, 3:208
- use of silencers, 3:81–82
- Office of the Surgeon General, U.S.
- biomedical effects of nuclear, biological and chemical weapons (NBC), 3:129–130
- Official Secrets Act, U.K. (1889, 1911, 1989), **2:382–384**
- Ogorodnik, Aleksander, 1:298
- Oil spills reporting, Coast Guard National Response Center, 1:223
- OIS. *See* Information Security, U.S. Office (OIS)
- Oklahoma City bombing, 1:134, 2:136, 3:144
- Olympic Games
- Munich 1972, 2:61, 2:283–284
- Salt Lake City 2002 security, 2:435
- Omnibus Diplomatic Security and Anti-terrorism Act (1986), 2:438
- OPEC. *See* Organization of Petroleum Exporting Countries (OPEC)
- Open market operations
- Federal Open Market Committee, 2: 13, 2:14
- Open source intelligence (OSINT), 1:199
- Operation Allied Force (Kosovo), 2:210
- Operation Desert Storm. *See* Persian Gulf War
- Operation El Dorado Canyon (Libya), 2:234
- Operation Enduring Freedom, **1:397–398**, 1:398
- Operation Engulf (U.K.), **1:404–405**
- Operation Green Quest, 1:296
- Operation Iraqi Freedom, 1:149, 2: 169, **2:169–176**
- aftermath of, 2:167–168



- aircraft in, 1:79, 1:80, 2:2
  - media coverage of, 2:175
  - missiles in, 1:285, 2:187
  - psychological warfare in, 2:109–110
  - shock and awe tactics in, 2:174
  - Operation Just Cause, 2:109
  - Operation Liberty Shield (Homeland Security), **2:385–386**
  - Operation Magic, **2:386–387**
  - Operation Mincemeat (WW II), 3:281–282, **3:282–283**
  - Operation Mongoose (Cuba), **2:387–388**
  - Operation Shamrock, **2:388–389**
  - Operation Torch (North Africa), 2:390
  - Operation Ultra, **3:184–185**
  - Operation Urgent Fury (Grenada), 1:29
  - OPIR. *See* Intelligence Policy and Review, U.S. Office of (OPIR)
  - Oppenheimer, J. Robert, 1:231, 2:23, 2:239, 2:246, 2:375
  - Orange Volunteers (OV), **2:389**
  - Organization of Petroleum Exporting Countries (OPEC), **2:384–385**
    - oil embargoes, U.S., 1:238, 2:384
    - U.S. national security and, 1:147, 2:315
  - Organized Crime Act (1970), 1:68
  - OSINT. *See* Open source intelligence (OSINT)
  - Ostrander, Sheila, 2:452
  - Ostrovsky, Victor, 1:157
  - Ottawa Convention (Land mine ban), 3:192
  - Ottoman Empire, 2:272–273
  - Outlying Area Reporting Station (OARS), 2:439
  - OV. *See* Orange Volunteers (OV)
- IP**
- P-3 Orion reconnaissance aircraft, **2:393**, 2:394
  - Pacific Northwest National Laboratory (PNNL), **2:394–395**, 2:395
  - PAGAD. *See* People Against Gangsterism and Drugs (PAGAD)
  - Painvin, Georges-Jean, 1:4
  - Pakistan, intelligence and security, **2:396–397**
  - Palestine Authority intelligence and security, **2:398**
  - Palestine Authority warfare summer camps, 2:75
  - Palestine Islamic Jihad (PLJ), **2:397**
  - Palestine Liberation Army (PLO), 1:1
  - Palestine Liberation Front (PLF), **2:397–398**
  - Palestine Liberation Organization (PLO), 1:61–62
  - Panama
    - Canal construction and history, 2:401
    - Noriega and intervention in, 1:30
    - Panama Canal Treaty, 2:401
    - Panama Canal, **2:401–403**, 2:402
      - U.S. transfer to Panama, 2:402
    - Panama Canal Commission, 2:402
    - Panama Canal Treaty, 2:401
    - PanAm Flight 103 bombing, **2:398–400**, 2:399
    - Parabolic microphones, **2:403**
    - Paranormal abilities, **2:451–453**
      - remote viewing experiments, 2:452
    - Para-state organizations, 3:151–154
    - Parks, Cliff, 3:277
    - Particle accelerators
      - at CERN, 1:171
    - Particle beam weapons, 1:399
    - Passenger screening
      - process, 1:21–22
      - for toxins, 1:5
    - Passive infrared systems (PIRs), 2:284–285
    - Pasteur, Louis, 1:81, 1:83
      - rabies vaccine, 3:223
    - Pasteurization, 1:81, 1:83
    - Pathogen genomic sequencing, **2:404**
    - Pathogens, **2:405–407**
      - transmission and spread of, 2:404–406
    - Pathogen transmission, **2:404–405**
    - Patriot Act, USA (2001), 1:386–387, 2:123, **2:408**, 2:409, 3:71
      - deterrence policy, 3:200
      - law enforcement intelligence under, 2:219–220
      - terrorist exclusion list, **2:407**
    - Patriot Missile System, **2:408–409**, 2:410
    - Payton, Gary (astronaut), 2:299
    - Pearl Harbor attack, 1:19, **2:410–413**, 2:411
    - Penicillin, 1:43
    - Penkovsky, Oleg, 2:281
    - Pennsylvania* (battle ship), 1:19
    - Pentagon, 1:350–351, 3:70
      - hacker attack on, 1:256
      - underground facility, 1:283
    - Pen Yen Yang, 1:373
    - People Against Gangsterism and Drugs (PAGAD), **2:413**
    - People’s Liberation Army (PLA, China), 1:189
    - People’s Republic of China (PRC). *See* China
    - Peron, Pres. Juan Domingo (Argentina), 1:52
    - Pershing, Gen. John
      - pursuit of Pancho Villa, 1:28
    - Persian Gulf War, **2:414–416**, 2:415
      - DIA intelligence in, 1:327
      - Kuwait oil fires, 2:213
      - news media and, 1:305
      - psychological warfare in, 2:109
      - stealth aircraft in, 1:80, 2:1
    - Personal security and identification
      - dumpster diving, 1:299–300, 1:342, 2:96
      - name recognition software, 2:94
    - Personal Status Monitor (PSM), 1:119–120
    - Personnel security
      - Personnel Security Investigations (PSI), 1:321–322
    - Peru
      - aircraft carrier development, 1:19
      - election protest in, 1:332
      - intelligence and security, **2:417**
    - Peterson, S., 2:256
    - Petroleum Reserve, U.S.
      - determination of, 2:417–419
      - Nixon and, 2:384
      - strategic, **3:125–126**
    - Petroleum reservoirs, 2:418–419
    - PFIAB. *See* President’s Foreign Intelligence Advisory Board (PFIAB)
    - PFLP. *See* Popular Front for the Liberation of Palestine (PFLP)
    - Pharmaceuticals
      - National Pharmaceutical Stockpile Program (NPS), 1:126, 1:319
    - Philby, Kim, 1:152, 1:152–153, 1:361, 2:203, 2:280
    - Philippines and the Spanish-American War, 3:102–103
    - Phoenix Program, **2:420–421**
    - Photo alteration, **2:421–423**
    - Photographic Interpretation Center, U.S. National (NPIC), **2:423–424**
    - Photographic resolution, **2:424**
    - Photography
      - digital alteration, 2:422–423
      - high-altitude, **2:424–426**
      - invention of, 1:419
      - traditional alteration, 2:421–422
    - PHS. *See* Public Health Service, U.S. (PHS)
    - Physics
      - electromagnetic spectrum, 1:381–382
      - nuclear, 2:375–376
      - spectrum, 1:382–383
    - Pickler, Nedra (reporter), 2:96
    - Pike, Otis (U.S. Congressman), 2:135
    - Pike Committee
      - congressional oversight of intelligence community, 2:135–136
    - Pincher, Chapman, 1:331
    - Pinkerton, Alan, 1:211, 3:207
    - Pinochet, Gen. Augusto (Chile), 1:29, 1:188
    - Planck, Maxwell, 2:294
    - Playfair, Lyon, 1:289, 2:426
    - PLF. *See* Palestine Liberation Front (PLF)
    - PLJ. *See* Palestine Islamic Jihad (PLJ)
    - PLO. *See* Palestine Liberation Army (PLO)
    - Plum Island Animal Disease Center, **2:427**, **2:427–428**
    - Plutonium, 1:231
      - fuel for nuclear fission, 2:23

- tracking nuclear materials, **3:255–257**
- PNNL. *See* Pacific Northwest National Laboratory (PNNL)
- Poindexter, John M., 2:156
- Poland
- intelligence and security, **2:428**
  - intelligence on Enigma cipher machine, 1:131–132
  - U.S.—Soviet relations in, 1:233
- Political murders
- by assassins or terrorists, 1:60–61, 2:34–35
- Pollard, Jonathan J. (espionage case), **2:430, 2:430–431**
- Polybius square, 1:3–4
- Polygraphs, **2:431–433, 2:432**
- Polygraph tests
- types of, 2:432
- Polymerase chain reaction (PCR), **2:433–436, 2:434**
- genetic detection devices, 1:117, 2:56, 2:379
- Pons, Stanley, 2:45
- Pony Express, 2:442
- Popp, Georg, 2:33
- Popular Front for the Liberation of Palestine (PFLP), **2:436–437**
- General Command (PFLP-GC), **2:437**
- Popular Movement for the Liberation of Angola (MPLA), 1:8
- Port Passenger Accelerated Security System (PORTPASS), **2:439–440, 3:67–68**
- Ports and Waterway Act (1972), 2:437–438
- Port security, **2:437–439**
- Port Security Units (PSUs), USCG, 2:438
- Portugal, intelligence and security, **2:440–441**
- Posse Comitatus Act (1878), 2:126
- Postal Reorganization Act (1970), 2:442
- Postal Service, U.S. (USPS), **2:442–443**
- emergency preparedness plan, 2:441–442
  - Postal security, **2:441–442**
- Potassium iodide, **2:443**
- Powell, Colin L.
- biological weapons in Iraq, 1:114
  - as Secretary of State, 1:325
  - United Nations Security Council and Iraq, 2:165
- Powers, Francis Gary, 1:76, 1:298–299, 2:425, 3:179–180, 3:181
- POWs. *See* Prisoners of war (POWs)
- Presidential candidates
- intelligence briefings of, **2:429**
- Presidential directives, 1:423, 2:309
- Presidential review memorandum forgery, 1:348
- President of the United States
- as executive commander of intelligence agencies, **2:444–445**
- President's Foreign Intelligence Advisory Board (PFIAB), **2:419–420, 2:445**
- Pretty Good Privacy (PGP), 1:228, 1:287, 1:291, **2:446**
- Primakov, Vyngeny, 1:148
- Prisoners of war (POWs), 2:125
- Privacy rights
- Bill of Rights, 2:447
  - Echelon, 2:448
  - Fair Credit Reporting Act (FCRA), 2:448
  - Freedom of Information-Privacy Acts (FOIPA), 2:447–448
  - legal and ethical issues, 2:447–448
  - Privacy Act (1974), 2:447
- Profiling, **2:448–450**
- Progressive Animal Welfare Society (PAWS), 2:249
- Prohibition Unit (ATF), 1:66
- Project GENETRIX, 1:93–94
- Projection radiography scanning, 3:51–52
- Project Shield America, 1:296–297
- Propaganda and psychological warfare
- Nazi propaganda, 2:451
  - uses and psychology, **2:450–451**
- protection of art and antiquities, 1:48
- Protein sequencing, 3:73
- Protocols of the Learned Elders of Zion forgery, 1:344–345
- Pseudoscience intelligence studies, **2:451–453**
- Psychic viewing, 2:452
- Psychological warfare, 2:108–109
- brainwashing, 2:209
- Psychotropic drugs, **2:453–455**
- Public buildings
- building risk assessment software (RAMPART), 1:49
  - designing for security, 1:48–50
  - government building design, 1:49
- Public communications
- Echelon monitoring, 1:370–372, 2:448
  - microchips for secure private, 1:218
- Public health response system, 1:248–252
- Public Health Service, U.S. (PHS), **2:455–456**
- Public safety
- Coast Guard (U.S. CG), 1:221–222
- Public surveillance
- closed circuit TV systems, 1:220–221
  - Echelon, 1:370–372
- Pueblo* incident, **2:456–458, 2:457, 3:77**
- Purification, air and water, 1:10–11, 1:127
- Purple machine (Japanese cipher machine), **2:459–460, 3:185**
- ## I Q I
- Qadhafi, Muammar, 2:233–234
- Quantum computing, 2:462–463
- Quantum cryptography, 2:462
- Quantum physics
- espionage and intelligence applications, **2:461–463**
  - nanotechnology and, 2:294–295
  - particle entanglement, 2:461–462
  - teleportation, 2:462–463
- QuickBird satellites, 3:44
- ## I R I
- R-7 ICBM (Soviet Union), 1:89
- Raborn, William F., Jr. 1:196, 1:310
- Radar, **3:1–2**
- doppler effect, 3:2, 3:119
  - satellites, 3:49
  - stealth technologies, 3:117–118
  - synthetic aperture, 2:59, 2:60, 3:2–3
- Radiation
- biological damage, **3:3–4**
  - for decontaminating, 2:244
  - detectors, 2:224, 2:362–363
  - energy absorption measurement of, 1:359
  - ionizing, 2:244
  - Large Volume Radiation Detector, 1:144
  - from nuclear weapons, 2:376
- Radioactive waste storage, 2:369–370, 2:381, **3:6–7**
- Radio equipment
- direction finding, **3:4–5**
  - radiometers for remote viewing, 1:390
  - RF detection, **3:23**
- Radio frequencies
- spectrum allocation, 1:383
  - waves as signals, 1:382
- Radio frequency (RF) weapons, **3:5–6, 3:23**
- Radiological Emergency Response Plan, U.S. Federal (FRERP), **3:8**
- Radio Tokyo, 3:163–164
- Al Rahman, Shaykh Umar Abd, 1:23
- Raman spectroscopy, 3:108–109
- Ranger* (aircraft carrier), 1:19
- Rasputin, Gregory Efimovich (Russian monk), 1:107
- Raymond, Michael, 2:280
- Reagan, Ronald
- Angolan support, 1:8
  - assassination attempt., 1:63, 3:56
  - Computer Security Act (1987), 1:261
  - Iran-Contra affair, 1:30, 1:279, 2:155–157
  - Operation Urgent Fury, 1:29
  - South African apartheid, 1:8
- Reagan administration (1981–1989)
- drug war, 1:313
  - missiles in Western Europe, 1:240
  - National Security Council, 2:358–359
  - national security policy, **3:9**
  - Strategic Arms Reduction Treaty (START), 3:9

- Strategic Defense Initiative (SDI), 1:42, 3:9
- Reagan signature forgery, 1:349
- Real IRA (RIRA), **3:10–11**
- Recombinant DNA, 2:56  
experiments, 1:57, 1:58  
genetic engineering of bacteria, 2:278–279, 2:406–407
- Recombinant DNA experiments. *See* Asilomar Conference
- Reconnaissance, **3:11**
- Reconnaissance aircraft  
Il'ya Mourometz bomber (Russian), 1:74  
Skunk Works (Lockheed Martin), 3:82–83  
SR-71 Blackbird, 1:76, 2:91, 2:425, 3:111–112  
U-2 spy plane, 1:74  
unmanned vehicles as, 1:76  
World War II, 1:75
- Reconnaissance satellites, 1:76, 2:248, 2:299
- Red Code (Japanese naval code), **3:12**
- Red Hand Defenders (RHD), **3:12–13**
- Red Orchestra, **3:13**
- Reid, John E., 2:433
- Reid, Richard, 3:77
- Reilly, Sidney, 2:262
- Reinsch, William (Commerce Dep't), 1:365
- Rejewski, Marian (Polish mathematician), 1:206, 1:407
- Remote sensing, **3:13–15**  
information source for terrain analysis, 2:59  
LIDAR system and images, 2:234–235, 3:14
- Remote sensing satellites, 1:187  
commercial, 3:43–45  
EM wave scanners, 1:392–393  
EROS satellites, 3:43  
IKONOS, 3:43  
Land Remote Sensing Policy Act, 3:43  
Landsat program, 2:425  
QuickBird satellites, 3:44
- Remote Video Inspection System (RVIS), 2:439–440
- Remote viewing, 2:452
- Renaissance, espionage in the, 1:418–419
- Reno, Janet, 1:358
- Republican Party resurgence, 1:233–234
- Republican Sinn Fein (RSF), 1:267
- Retina and iris scans, **3:15–17**
- Revenue Acts (1916, 1917), 3:170
- Revolutionary Armed Forces of Colombia (FARC), **3:18**
- Revolutionary Nuclei, **3:18**
- Revolutionary Organization 17 November (17 November), **3:19**
- Revolutionary Organization of Socialist Muslims. *See* Abu Nidal Organization (ANO)
- Revolutionary People's Liberation Party / Front (DHKP/C), **3:19**
- Revolutionary Proletarian Initiative Nuclei (NIPR), **3:20**
- Revolutionary United Front (RUF), **3:20**
- Revolutionary War, American, 2:74, 3:06, **3:21–23**
- Rewards for Justice Program, 1:276, 3:153
- Rice, Condolezza, 2:309, 2:359
- Richardson, Bill (U.S. Energy Secretary), 1:191
- Richelson, Jeffrey T. (writer), 1:197, 1:372
- Ricin, 1:107, **3:24**, 3:166–167
- Ridge, Tom (Homeland Security director), 1:124, 2:86, 2:359  
Operation Liberty Shield, 2:385–386
- Ridgway, U.S. Gen. Matthew B., 2:208
- Rintelen, Franz von, 1:130
- Rivest, Ronald, 1:286
- Robotics  
brain-machine interfaces for, 1:140  
energy harvesting and, 3:26–27  
spacecraft and, 3:26  
vehicles, **3:25–27**
- Rogers, William, 2:358
- Rohrbacher, Dana, 3:42
- Roman Empire  
espionage in the, 1:416–417
- Romania, intelligence and security, **3:27–28**
- Romerstein, Herbert, 1:349–350
- Roosevelt, Franklin D., 1:198, 1:230
- Roosevelt, Theodore  
Rough Riders in Spanish-American War, 3:103
- Rosario Cases, Maria Del, 1:31
- Rosenberg espionage case (Ethel and Julius), 3:29, **3:29–30**
- Rossignol, Antoine, 1:128
- Rostow, Walt, 2:189
- Rover race (DARPA sponsored), 1:306
- Rowan, Andrew, 3:103
- Rowley, Colleen, 3:71
- Royal Canadian Mounted Police (RCMP), 1:160, 1:161  
National Drug Intelligence Estimate (NDIE, Canada), 1:363
- Royal Navy (U.K.), 1:19
- RPF. *See* Rwandan Patriotic Front (RPF)
- RQ-1 predator aircraft, 1:27
- Rubin, Robert, 3:170
- Rugova, Ibrahim, 2:211
- Rumsfeld, Donald H., 2:170, 2:359
- Rusk, Dean, 1:325, 2:189, 2:198
- Russia  
aerial reconnaissance, 1:74  
aircraft carrier development, 1:19–20  
art and antiquities looting during 1917 Revolution, 1:46  
Chechnya-Russian conflict, 1:172–173  
intelligence and security, **3:30–31**  
nuclear materials security issues, **3:31–33**, 3:38  
Nunn-Lugar Threat Reduction Program, 3:32  
Russian-Chechen referendum, 1:173  
*See also* Soviet Union
- Rutherford, Ernest, 2:294
- Rwanda  
genocide in, 1:7  
terrorists in, 1:55
- Rwandan Patriotic Front (RPF), 1:7

## ISI

- Sabotage, 3:35, **3:35–36**
- Sadat, Pres. Anwar (Egypt), 1:59, 1:331
- Safe Streets Act (1968), 2:195
- Safire, William, 3:42
- Sagan, Carl (scientist, 1934–1996), 2:376, 2:378
- Salafist Group for Call and Combat (GSPC), **3:36**
- Salmon, Daniel, 3:37
- Salmonella and salmonella food poisoning, **3:37–38**
- Sandia National Laboratory (SNL), 2:241, **3:38–39**, 3:39  
vulnerability assessments, 3:245
- Sanni, Violetta, 3:74–76
- Santos-Dumont, Alberto (airship designer), 1:93
- Sarin gas, 3:40, **3:40–41**
- SARS. *See* Severe Acute Respiratory Syndrome (SARS)
- Satellite imagery  
monitoring accident sites, 1:187  
remote sensing, 1:187, 2:425, 3:43–45
- Satellites  
commercial, 3:43–45  
digital cameras in, 2:423  
dual use technology, 1:364  
Echelon, 1:370–372, 1:386  
KH series surveillance cameras, 1:155–156  
non-governmental, high resolution, 3:43, **3:43–45**, 3:44  
nuclear device mishaps, 2:319–320  
remote sensing, 1:187, 2:425, 3:43–45  
space debris impact risk, 2:319  
spy satellites, 1:187, 2:248
- Satellite technology  
altimetry measurements for bathymetric maps, 1:96  
exports to the People's Republic of China, **3:41–42**  
radar, 3:49  
telemetry intelligence (TELINT), 3:48
- Saudi Arabia, 3:44  
Arab-Israeli wars, 2:273  
intelligence and security, **3:50–51**
- Savimbi, Jonas, 1:8

- SBCCOM. *See* Soldier and Biological Chemical Command, U.S. Army (SBCCOM)
- SBIRS. *See* Space-Based Infrared Satellite Systems (SBIRS)
- Scanning and scanners  
backscatter imaging, 3:53  
coherent scattering, 3:53  
computer tomography, 1:135, 3:52  
EM wave scanners, 1:392–393  
projection radiography, 3:51–52  
retina and iris, 3:15–16  
stereoscopic x-ray screening, 3:53
- Scanning technologies, **3:51–53**, 3:52
- Scanning tunneling microscopes, 2:271
- Schabowski, Guenter, 1:106
- Schaefer, Vincent Joseph, 2:259
- Scherbius, Arthur (Enigma inventor), 1:205, 1:291, 1:405
- Schlessinger, James R., 1:310
- Schlieren system, 1:16
- Schrader, Gerhard (chemist), 2:321–322
- Schrödinger, Erwin, 2:295
- Schroeder, Lynn, 2:452
- Schulmeister, Charles, 2:297–298
- Schwarzkopf, Gen. H. Norman, 2:414
- Schweitzer-Pinochet letter forgery, 1:349
- Science fiction media  
Area 51, 1:51  
movies, 2:288–289
- Scotland Yard, 3:194
- Scowcroft, Lt. Gen. Brent (security advisor), 2:30, 2:358  
Clinton intelligence briefing, 2:429
- Scramjet engines, 2:91–92
- SEAL teams, **3:53–54**, 3:54, 3:55
- Search and rescue programs, 2:341
- Secret Intelligence Branch (SI, OSS), 2:390
- Secret Service, U.S., **3:55–57**, 3:56
- Secret writing, **3:58–59**, 3:59  
steganography, 3:119–120
- Secure Electronic Network for Travelers' Rapid Inspection (SENTRI), 2:439, **3:67–68**
- Security, Infrastructure Protection and Counter-terrorism, U.S. National Coordinator, **3:62**
- Security cameras, 1:156  
closed circuit television systems, 1:219–220  
perimeter security video and TV systems, 1:219–220
- Security clearances  
investigations, 1:322, **3:59–62**  
levels of, 3:60  
procedures for, 3:61–62
- Security equipment  
cameras, 1:156  
closed circuit television systems, 1:156  
DNA signatures, 1:342  
motion sensors, 2:284–285  
*See also* Security cameras
- Security Oversight Board, 1:209
- Security personnel, 2:4
- Security Policy Board, U.S., **3:63**
- Security systems  
Closed circuit television systems (CCTV), 1:219–221  
LoJack auto security and GPS, 2:69  
procedures and equipment, 2:4–5  
video motion detectors, 1:219
- Seismology  
forensic science, 2:35  
monitoring explosions, **3:65**  
Seismograph, **3:63–64**
- Selassie, Haile (Ethiopian emperor), 1:7
- Select Intelligence Committee (U.S. Senate). *See* Church Committee
- Senate Intelligence Committee (U.S.), 1:32–33, 1:202
- Senate Select Committee on Intelligence (U.S.), **3:66**
- Senate Watergate committee, 3:253, 3:254
- Sendero Luminoso (Shining Path, or SL), **3:66–67**
- September 11 terrorist attacks, 1:26, 1:196, **3:68–72**, 3:69, 3:70  
aftermath, 1:34–36  
Bush, U.S. Pres. George W., 1:148, 3:70  
CIA and, 1:201  
emergency responses to, 3:70  
FBI and, 3:71  
international reactions to, 3:71  
*See also* Pentagon; Terrorist attacks; World Trade Center
- Sequencing, **3:72–73**
- Serbia, intelligence and security, **3:73–74**
- Sergeyev, Igor (Russian defense minister), 1:173
- Severe Acute Respiratory Syndrome (SARS), 1:248–252  
quarantine legislation for, 1:251
- Sex-for-Secrets scandal, **3:74–76**, 3:277
- Shamir, Adi, 1:286
- Shayler, David, 2:383
- Shepardson, Whitney H., 2:390
- "Shoe bomber," **3:77**
- Shoe transmitter, 3:78, **3:78**
- Short-wave transmitters, **3:78–79**
- Shuttle Radar Topography Mission, 2:248
- Sicherheitsdienst (Nazi Security Service), 1:2
- Sierra Leone, funding for civil war, 1:8
- SIGINT (Signal Intelligence), **3:79–80**  
sources, 1:193  
use in Korean war, 2:209  
Venona monitoring Soviet diplomatic communications, 3:228–231
- Signal Intelligence Service (SIS, U.S. Army), 1:243–244, 2:390  
Operation Magic, 2:386–387  
Operation Shamrock, 2:388–389  
Venona Project, 3:228–231, 3:229
- Silencers (guns), **3:80–82**, 3:81
- Sims, William, 3:103
- Skunk Works (Lockheed Martin), **3:82–83**, 3:83
- Sleep deprivation, countermeasures, 1:270
- Slovakia, intelligence and security, **3:83–84**
- Slovenia, intelligence and security, **3:84**
- Smallpox, **3:84–85**  
as a biological weapon, 1:124  
science facilities for, 1:169  
vaccination for, 2:103, 3:86  
variola virus, 3:226–227
- SMERSH (KGB assassination team)  
Leon Trotsky, 1:61  
poison pistols used by, 1:63–64
- Smith, David L., 2:245
- Smith, Don, 1:308
- Smith, Gen. Walter Bedell, 1:195
- Smith Act (1940), 2:7
- Sniffer dogs, 1:164–165
- Socialist Party (U.S.)  
and Espionage Act (1917), 2:122
- Socrates (c. 479–399 B.C.), 1:106
- Sokolski, Henry, 3:42
- Soldier and Biological Chemical Command, U.S. Army (SBCCOM), **3:88–89**
- Solzhenitsyn, Aleksandr, 1:3
- Somalia, 1:7  
Al-Ittihad al-Islami (AIAl), 1:24  
Operation Restore Hope, 1:6
- Soman (nerve gas), **3:89–90**
- Somoza Garcia, Anastazio, 1:28
- Sonar, **3:90–91**
- Sorenson, Paul S., 2:316
- Sound surveillance system (SOSUS), **3:91–92**
- South Africa intelligence and security, **3:92**
- South African apartheid, 1:8
- Southeast Asian Treaty Organization (SEATO), 1:237, 1:379
- South Korea. *See* Korea, South
- Soviet Union  
Afghanistan invasion, 2:358  
Antiballistic Missile (ABM) Treaty, 1:41–42  
Berlin blockade, 1:99–101, 1:103  
Cambridge University Spy Ring, 1:151–155, 3:96  
Cuban Missile Crisis, 1:29, 1:293–295  
disinformation in, 1:332–333, 2:203  
Glasnost and anti-communism movements, 1:241  
high power microwave weaponry, 2:272  
intelligence and security, 1:75, 3:76–77, **3:93–96**, 3:230–231  
Iran crisis, 1:231  
jet aircraft in, 1:75  
KGB, 1:102, 1:280–281, 1:331, 3:95–96  
Marine mammal program, 2:249  
Nixon's visit to China, 2:335



- political parties and free elections in, 1:241
- R-7 ICBM, 1:89
- space stations, 3:97
- Sputnik 1, 1:237
- Strategic Arms Limitation Talks (SALT), 2:335
  - WW II U.S. relations with, 1:230–231
- Space-Based Infrared Satellite Systems (SBIRS), 3:49
- Spacecraft, 3:83
  - Institute of Future Space Transport concept, 2:91
  - Sputnik 1 (Soviet Union), 1:89, 1:237
- Space debris
  - causes of, 2:320
  - cleanup options, 2:319, 2:321
  - collision avoidance, 2:320–321
  - in Earth orbit, 2:319–321
  - NORAD tracking, 2:345
- Space environment
  - meteors as hazard in, 2:320
  - space debris impact risk, 2:319
- Spaceflight early piloted flights, 1:89
- Spacelab, 3:98
- Spaceplanes, 3:99
- Space shuttle
  - DOD payloads on, 2:299
  - military, 3:99
  - mission of, 2:299
  - orbiter, 3:97–98
  - propulsion systems, 3:98
  - Shuttle Radar Topography Mission, 2:248
  - Spacelab payloads, 3:98
- Space shuttle Challenger, 2:299, 3:99–100
- Space shuttle Columbia, 2:299
  - accident analysis, 1:259, 3:48, 3:100
  - GIS debris field mapping, 2:65
- Space shuttle program, **3:96–100**
- Space Stations, 3:97
- Spain
  - aircraft carrier development, 1:19
  - First of October Anti-facist Resistance Group (GRAPO), 2:20
  - guerilla warfare by partisans, 2:74
  - intelligence and security, **3:101**
- Spanish-American War, **3:101–103**, 3:102
- Special Anti-narcotics Force (Bolivia), 1:133
- Special Collection Service, U.S., **3:103–104**
- Special Operations Command, U.S., **3:105**
- Special Operations Executive, U.K. (SOE), **3:87–88**
- Spectrometry
  - air plume analysis, 1:16–17
  - mass, 2:38
- Spectroscopy, **3:107–109**
  - detection methods, 1:175, 1:184
  - nuclear activation analysis, 2:373
- Spectrum, 1:382–383
- Spertzel, Richard (U.N. weapons inspector), 1:334
- Spores, 3:109, **3:109–111**, 3:244–245
- SPOT satellite program, 1:187, 2:60
- Sputnik 1 (Soviet Union), 1:89, 1:237, 2:298
- Spy-in-the-sky intelligence, 1:237
  - satellite surveillance, 3:46
  - Soviet-Cuban missile emplacements, 1:196
  - spy planes, 1:197, 3:180–182
- Spy novels, 2:130–132
- Spy rings
  - Cambridge University Spy Ring, 1:151–155
  - Walker family spy ring, 3:249
- Spy satellites, 1:197, 3:45, **3:45–50**
  - Air Force SAMOS and MIDAS satellites, 3:47
  - CORONA, 2:425, 3:46–47
  - DSP satellites, 2:427–248
  - film retrieval in reentry capsules, 3:46
  - KH “keyhole” series, 1:187, 1:310, 3:15, 3:46, 3:48
  - Soviet Union’s, 3:47–48
  - types of intelligence from, 2:248, 3:48–49
- SR-71 Blackbird, 1:76, 2:91, 2:425, **3:111–112**, 3:112, 3:116
- Stalin, Joseph (1879–1953), 1:230, 1:231, 2:207
  - Cold War declaration, 1:233
  - death of, 1:235
- Star Wars (SDI). *See* Strategic Defense Initiative (SDI)
- STASI (East German intelligence agency), **3:114–115**, 3:115
- State Department, U.S., 1:55, **1:324–326**
  - bureaus and offices, 1:326
  - Coordinator for Counter-Terrorism, 1:270–271
  - intelligence agencies in, 3:204
  - Secretaries of State, 1:325
- Stealth technology, **3:115–119**, 3:316
  - B-2 Bomber, 1:79
  - F-117A Stealth Fighter, 2:2
- Steganography, **3:119–120**
- Stereoscopic scanning
  - x-ray screening, 3:53
- Sterilization, 2:244
- Stevenson, Adlai, 1:98
- Stieber, Wilbur, 1:2
- Stockpile Stewardship and Management Program (SSMP), 2:225
- Straight, Michael, 1:154
- Strassman, Fritz, 2:22, 2:375
- Strategic Air Command, U.S. (SAC), 2:237
- Strategic Arms Limitation Talks (SALT), 1:76, 1:238, 2:335
- Strategic Arms Limitation Treaty (SALT II), 1:166–167
- Strategic Arms Reduction Treaty (START), 1:76, 1:240, 2:377, 3:9, **3:112–313**
- Strategic Arms Reduction Treaty (START II), **3:113–314**
- Strategic Command, U.S., **3:220**
- Strategic Defense Initiative (SDI), 1:121, 1:240, 3:9, **3:120–125**
- Stun guns
  - Taser, 3:134–135
- Sturgeon* (U.S. submarine), 3:188–189
- Submarines
  - espionage and the use of, **3:188–190**, 3:189
  - sonar for underwater navigation, 3:90
  - Soviet, 3:189–190
  - United States, 3:188–189
- Substance Abuse and Mental Health Services Administration (SAMHSA), 2:455
- Sudan, U.S. attacks on, 2:274
- Sudan intelligence and security, **3:126**
- Suez Canal, 1:404–405, **3:127**
- Sung Li, 1:373
- Supercomputers, **3:128**, 3:129
- Surveillance cameras, 1:155–156
  - copy and robot cameras, 1:156–157
  - in Eastern Europe, 1:156
  - See also* Reconnaissance aircraft; Reconnaissance satellites
- Surveillance systems
  - closed circuit TV systems, 1:220–221
  - Echelon, 1:370–372, 1:386
- Sutcliffe, R.C., 2:256
- Sverdlovsk, Russia, 1:235
- Sweden, intelligence and security, **3:130**
- Switzerland, intelligence and security, **3:131**
- Symington, W. Stuart, 1:13
- Synge, Richard, 2:49
- Synthetic aperture radar (SAR), 2:59, 2:60, **3:2–3**, 3:14
- Syria, intelligence and security, **3:131–132**
- SZ42 Cipher, 1:205
- Szilard, Leo, 1:231, 2:246

## I T I

- Tabun (nerve gas), **3:133**
- Taft-Hartley Act (1947), 2:122
- Taiwan
  - intelligence and security, **3:134**
  - Tachen Straits crisis, 1:237
- Taliban and Al-Qaeda (Afghanistan), 1:27, 2:125, 2:274, 3:68
- Tanaka memorandum forgery, 1:346–347
- Tariff Act (1789), 1:296
- Taser, **3:134–135**, 3:135
- Taxpayers, protection of rights, 2:137
- TCG (Tunisian Combatant Group), **3:175**
- Technical intelligence (TECHINT), **3:136**
- Technology

- preventing counterfeit currency, 1:274
- Technology Applications Program (BMDO), 1:86
- Technology sharing between U.S. and U.K., **3:106–107**
- Technology Transfer Center, National (NTTC), **3:136–137**
- Telecommunications policy
- National Security Telecommunications Advisory Committee, 2:311
  - National Telecommunications Information Administration, U.S. (NTIA), 2:312
  - Telecommunications Act (1996), 2:10
- Telegraph
- cryptography and the, 1:419
  - foreign transmissions monitored, 2:388–389
- Telemetry, **3:137**
- Telephone Caller Identification (Caller ID), **3:137–138**
- Telephone recording laws, **3:138**
- Telephone recording system, **3:139**
- Telephone scrambler, **3:139**
- Telephone tap detector, **3:140**
- Teller, Edward, 2:375
- TEMPEST technology
- as electronic intelligence, 1:385
- Tenebaum, Ehud, 1:256
- Tenet, George J., 1:194, 1:196, 1:311, 1:328, 2:168
- Terrain intelligence, **2:58–59**
- Terror alert system, U.S., **3:140–142**, 3:141
- Terrorism, domestic (U.S.), **3:142–146**
- Terrorism, history and ideology
- anarchism as ideological force, 3:148
  - philosophical origins, **3:148–150**, 3:149
- Terrorism, intelligence based on
- Australian intelligence, 1:72
  - computer and internet technologies aiding, 2:8–9
  - drug traffic and narco-terrorism, 1:281, 1:314
  - financial intelligence, 3:157–158
  - GAO threat and risk assessment report, **3:146–147**, 3:147
- Terrorism Act (U.K.), **1:142**
- Terrorist attacks
- bombings, 1:48
  - CIA and, 1:201
  - domestic, 2:126
  - drug traffic and narco-terrorism funding, 1:281, 1:314
  - terrorism risk insurance, 3:151
  - See also* September 11 terrorist attacks; World Trade Center
- Terrorist Information Awareness (TIA) system, 1:22, **3:162**
- Terrorist organizations
- use of asymmetric warfare, 1:68
  - financing of, 3:157–158
  - freezing of assets, **3:155–160**
  - international, 1:1
  - nuclear materials trafficking reported, 3:32
  - para-state organizations, **3:151–154**, 3:152, 3:153
  - state-sponsored, 3:154
  - Terrorist organization list, U.S., **3:154–155**
- Terrorist Threat Integration Center, 1:149, **3:160–161**
- Teten, Howard, 2:449
- Tethered Aerostat Radar System (U.S. Air Force), 1:94
- THAAD. *See* Theater High Altitude Area Defense (THAAD)
- Thailand, 1:19
- Theater High Altitude Area Defense (THAAD), 1:86
- Think tanks, 2:342
- Thin layer chromatography, 2:38, **3:161–162**
- Thithmius (16th century German monk), 1:289
- Thomson, Sir J.J., 2:49, 2:294
- Three Mile Island nuclear accident, 2:24, 2:372
- Threshold Test Ban Treaty, 1:253–254
- Thyroid gland cancer therapy, 2:443
- TIA. *See* Terrorist Information Awareness (TIA); Total Information Awareness (TIA)
- Tiselius, Arne, 1:391
- Tissue-based biosensors, **3:163**
- Tissue engineering, 1:111–112
- Toguri, Iva Ikoku, 3:163–164
- Tokyo Rose, 2:450, **3:163–164**
- Tolbert, Pres. William (Liberia), 1:8
- Tolman, Dr. Richard, 2:246
- Tomahawk cruise missile, 1:284–285
- Tomography
- computer, 1:22, 1:135–136, 3:52
- Topography and topographic maps, 2:248
- military use of terrain intelligence and, 2:58–59
  - radar mapping, 2:59
  - Shuttle Radar Topography Mission, 2:248
- Torpedoes, in Civil War, 1:211
- Torture techniques and technologies, **2:152–155**, 2:153
- Total Information Awareness (TIA), 1:22, 2:146
- Tournament of Shadows, 2:71–72
- Townsend, Robert, 3:22
- Toxicology, **3:164–165**
- Toxic spills reporting
- Coast Guard National Response Center, 1:223
- Toxic Substances and Disease Registry, Agency for (ATSDR), 2:455
- Toxins, **3:166–167**
- Anthrax, 1:33–34
- APS analysis of toxin structure, 1:53
- mapping concentration and distribution of, 1:113
- vaccines for, 3:167
- Trade craft, **3:167**
- Trading with the Enemy Act (1941), 3:171
- Traffic surveillance system, 1:357
- Transportation Department, U.S., 3:168, **3:168–169**
- intelligence agencies in, 3:204
- Transportation Security Administration (TSA)
- airport screeners, 1:77–78
  - aviation security in U.S., 1:209, 3:72
  - Federal Air Marshalls, 1:14
- Treasury Department, U.S., **3:169–171**, 3:170
- freezing of terrorist assets, 3:155–156
  - international monetary policy (post WW II), 3:171
  - Operation Green Quest, 3:158
- Treaty of Versailles, 2:226
- Tritium, 2:81–82
- Trotsky, Leon, 1:61
- Trudeau, Pierre Elliot (Canadian Prime Minister), 1:162
- Truman administration (1945–1953), 1:200
- atomic bomb use on Japan, 1:231
  - Cold War policy and Truman Doctrine, 1:231–232, 1:233, 3:172
  - hydrogen bomb request, 1:232
  - national security policy, **3:171–172**
- Truth serum, **3:173–174**
- TSA. *See* Transportation Security Administration (TSA)
- Tularemia (disease), **3:174–175**
- Tunisian Combatant Group (TCG), **3:175**
- Tunisian Islamic Fighting Group, 3:175
- Tunner, Maj. Gen. William H., 1:100
- Tupac Amaru Revolutionary Movement (MRTA), **3:175**
- Turing, Alan
- cryptography and Enigma, 1:407, 3:184
  - Turing bombe development, 1:137, 1:206, 1:242
- Turkey, intelligence and security, **3:176**
- Turkish Hizballah, **3:176**
- Turner, Admiral Stansfield, 1:310
- TV shows
- espionage and intelligence portrayals, 2:288–289
  - Get Smart*, 3:78
- Typex cipher machine, **3:177**
- U-2 spy plane (U.S.), 1:74, 1:237, **3:180–182**, 3:181
- design of, 3:182

- Russian capture of, 1:76
- U-2 incident, **3:179–180**
- UAV. *See* Unmanned Aerial Vehicles (UAV)
- See also* U-2 spy plane (U.S.)
- Ukraine, intelligence and security, **3:183**
- UKUSA. *See* United Kingdom—United States of America Security Agreement (UKUSA)
- Ullman, Harlan K et. al.
  - Shock and Awe: Achieving Rapid Dominance*, 2:107
- Ulster Defense Association (UDA), **3:183**
- Ulster Freedom Fighters (UDA/UVF), **3:183**
- Ultra, Operation, **3:184–185**
- Ultra-high pressure sterilization, 2:244
- Ultraviolet spectroscopy, 3:107–108
- Ultraviolet waves, 1:383
- Un-American Activities Committee, U.S. House (HUAC), 2:122–123, 2:252
- Underground facilities, U.S. Government, **3:186–188**, 3:187
- UNESCO. *See* United Nations Educational, Scientific and Cultural Organization (UNESCO)
- Unexploded ordnance and mines. *See* Land mines clearance programs; Munitions, unexploded ordnance clearance programs
- Unidentified flying objects (UFO's)
  - Area 51, 1:51
  - government study of, 1:75
- Union balloon corps (Civil War, U.S.), 1:92
- UNITA. *See* National Union for the Total Independence of Angola (UNITA)
- United Airlines, hijacked flights—9/11, 3:69
- United Kingdom
  - aircraft carrier development, 1:19
  - assassination attempts on N. Bona parte, 2:297
  - Berlin Airlift operations, 1:100
  - counter-terrorism policy, **3:193**
  - D Notice system, 1:305
  - espionage in 19th century France, 2:296–298
  - intelligence and security, **3:194–195**
  - intelligence on Iraqi weapons programs, 2:167–168
- United Kingdom—United States of America Security Agreement (UKUSA), 3:106–107
- United Nations
  - blocking terrorist financing, 3:158–159
  - Security Council, **3:196–198**, 3:197
  - war crimes tribunal, 2:211
- United Nations Educational, Scientific and Cultural Organization (UNESCO)
  - protection of artifacts convention, 1:47
- United Nations Security Council
  - China and, 1:189
- Iraq and Resolution 1441, 2:164
- Resolution 1373, 1:160–161
- United Self-Defense Forces/Group of Colombia (AUC), **3:198**
- United States
  - America enters World War II, 3:279–280
  - bombing of embassy and barracks in Lebanon, 2:227–228
  - counter-terrorism policy, **3:198–201**, 3:199
  - Cuban Missile Crisis, 1:29
  - hostages in Iran, 1:166
  - OPEC and Middle East oil dependency, 1:166, 1:238
- U.S. Army
  - Operation Sea Spray, 1:118
  - School of the Americas, 1:29
- U.S. Atomic Energy Detection System (USAEDS), 1:12–13
- U.S. Congress
  - classified information leaked from, 1:214
  - oversight of Intelligence community, 2:130, 2:135–136
- United States elections
  - Civil Rights Commission study on Florida balloting of Nov. 2000, 1:247–248
- United States foreign policy
  - containment of Soviet expansionism, 2:189, 2:206–207
  - Monroe Doctrine and, 2:281–282
  - State Department and, 1:325
- United States intelligence and security, 3:202–205
  - Chinese espionage in, 1:190–191
  - CIA foreign intelligence, 1:193
  - dawn of professional, 3:207–208
  - domestic, 1:192
  - Foreign Intelligence Advisory Board, 1:194
  - history of, **3:206–209**
  - intelligence history and historical records, 1:197
  - intelligence sources, 1:193
  - Senate Select Committee on Intelligence, 1:192, 1:194
  - See also* CIA
- United States military
  - bombing of U.S. marine barracks in Lebanon, 2:227–228
  - Reagan's buildup of, 1:240
- United States security policy and interventions
  - Africa, 1:5–9
  - Latin America, 1:28–31
- United States—Soviet relations
  - capitalism vs. socialism, 1:232, 1:233
  - Cold War, 1:230–232
  - Nixon's arms reduction talks, 1:238
  - in Poland, 1:233
- United States Special Forces
  - in Afghanistan, 1:60
- Delta Force, 1:322–323
- United States technology
  - Chinese interest in, 1:191
  - dual use technology, 1:364–365
  - Eisenhower's innovation policy, 1:235
  - source literature on, 1:191
- Unmanned Aerial Vehicles (UAV), **3:209–210**, 3:210
  - as reconnaissance aircraft, 1:27, 1:51, 1:76
- Uranium, **3:211–212**, 3:212
  - converted to commercial use, 1:355
  - depletion weapons, 1:333–334, **3:212–213**
  - nuclear fission using, 2:22–23
- Uranium, weapons grade, 1:231
  - enrichment processing facility, 1:235
  - tracking nuclear materials, **3:255–257**
- Urbani, Dr. Carl (SARS identification), 1:249
- USAEDS. *See* U.S. Atomic Energy Detection System (USAEDS)
- USAMRIDC (Medical Research Institute of Chemical Defense, U.S. Army), **3:213–214**
- USAMRIID (Medical Research Institute of Infectious Diseases, U.S. Army), 3:214, **3:214–216**
- USCSB. *See* Chemical Safety and Hazard Investigation Board (USCSB, U.S.)
- USS *Cole*, **3:216–217**
- USS *Liberty*, **3:218–220**, 3:219
- USS *Maine* sunk near Cuba (1888), 3:101–102, 3:102
- USSTRATCOM. *See* Strategic Command, U.S.

**V**

- V-2 ballistic missile, 1:87, 1:89
- Vaccination, **3:221–222**
- Vaccine development
  - at Brookhaven National Laboratory, 1:143
  - at FDA, 2:10–11
  - production and, 3:224–225
- Vaccines, **3:223–226**
  - anthrax, 1:37–39, 1:39, 3:221
  - genetic engineering of, 3:86
  - livestock, 2:427
  - rabies, 3:223
  - Salk polio, 1:168, 1:170, 3:224
  - smallpox, 2:103, 3:85, 3:86, 3:223
  - storage, 2:427
  - toxins, 3:167
- Vanunu, Moredechai, 2:182
- Variola virus (smallpox), 3:84, **3:226–227**
- Venezuela, intelligence and security, **3:227–228**
- Venona, **3:228–231**, 3:229
- Vernam, Gilbert, 1:207, 1:242, 1:291

- Vibrational spectroscopy, 3:108–109  
 VICAP. *See* Violent Criminal Apprehension Program (VICAP)  
 Victims of Crime Act (1984), 2:195  
 Viet Minh (League for the Independence of Vietnam), 3:231  
 Vietnam  
   Army Security Agency (ASA, U.S.), 1:56  
   escalation of U.S. involvement in, 2:189  
   first to control SARS outbreak, 1:251  
   Geneva Accords division of, 3:232  
 Vietnam, South  
   Phoenix Program operations in, 2:420–421  
   U.S. support of, 2:188  
 Vietnam War, **3:231–236**, 3:232, 3:233  
   Agent Orange, 1:9–10  
   Agent Orange used in, 1:9–10  
   beginnings of, 1:237  
   CIA involvement in, 3:234–235  
   napalm attacks by U.S., 1:181  
   Nixon's pull-out from, 2:334, 3:234  
   Tet Offensive, 3:233–234  
   Tonkin Gulf Resolution, 2:189, 3:233  
   U.S. loss of S. Vietnam to communists, 2:30, 3:234  
 Vigenere, Blaise de, 1:289  
 Villa, Pancho, 1:28  
 Violent Criminal Apprehension Program (VICAP), 2:449–450  
 Viral biology, **3:236–240**, 3:237  
 Viral exposure therapy, antiviral drug development, **3:241**  
 Virology, 3:236–238  
   anti-viral drug development, 3:241  
 Virtual reality modeling language (VRML), 1:259  
 Viruses  
   identification of, 3:238  
   replication, 3:239–240  
 Visible light waves, 1:382–383  
 Voice alteration, electronic, **3:242**  
 Voice analysis, 2:39–40  
 Voice of America (VDA), U.S., 3:243, **3:243–244**  
 Vonnegut, Bernard, 2:259  
 Vozorzhdneniye Island (Russia) biochemical weapons test facility, **3:244–245**  
 Vulnerability assessments, **3:245**  
 VX agent, **3:246–247**
- I W I**
- Walker, Jr., John A., 1:159, 1:275, 1:361, 3:249  
 Walker, Michael Lance, 3:249  
 Walker, William, 1:28  
 Walker family spy ring, 2:280, **3:249**  
 Wallis, John, 1:128  
 Ward, Henry, 3:103  
 Warner Brothers spy movies, 2:287
- War of 1812, **3:250–251**  
 War Powers Act of 1973 (Bolland Amendment), 1:30  
 Warren, David, 2:25  
 Wartime plunder, 1:45–48  
 Washington Naval Limitation Treaty (1922), 1:19  
 Watergate break-in, 1:202, 2:28, **3:253–254**  
 Water supply  
   contamination/decontamination, 1:10–11, **3:251–252**  
   counter-terrorism threat to, 3:251–253  
   EPA monitoring, 1:127  
 Weapon inspections  
   Iran, 2:161  
   Iraq, 2:163–166  
 Weapons  
   bludgeons and blunt instruments, 1:64  
   Confederate infernal, 1:211  
   energy directed, 1:399  
   knives and edge weapons, 1:64  
 Weapons of mass destruction (WMD), **3:257–259**  
   detection, **3:260–263**  
   Iraq, 2:167–168, 2:169–176  
 Weather alteration, 2:259–260  
   cloud seeding, 2:257, 2:259–260  
 Weather forecasting  
   National Weather Service, 2:257  
   types of forecasting, 2:258–259  
   weather and Doppler radar, 2:256–257, 2:257  
 Weathersby, Katherine, 1:332  
 Webster, Daniel W.  
   *Comprehensive Ballistic Fingerprinting of New Guns*, 1:85  
 Webster, William H., 1:196, 1:311, 2:8  
 Weinberger, Casper W., 2:156–157, 2:358  
 Weinberger SDI speech forgery, 1:348–349  
 Weitling, Wilhelm (1808–1871), 3:150  
 Welch, Joseph, 2:253  
 Wen Ho Lee, 1:190, 1:191, 1:213, 2:133  
 Westmoreland, Gen. William C., 3:233  
 West Nile virus, 2:104  
 Whalen documents forgery, 1:347  
 Wheatstone, Sir Charles, 2:426  
 Whistleblower protections  
   cases, 3:105  
   Office of Special Counsel (OSC), **3:104–105**  
   Whistleblower Protection Act (1989), 3:104  
 Whitworth, Jerry Alfred, 3:249  
 WHO. *See* World Health Organization (WHO)  
 Wickham, William, 2:296  
 Wilson, Vice Admiral Thomas R., 1:303, 1:328  
 Wilson, Woodrow  
   League of Nations and Nobel Peace Prize, 2:226  
 Windtalkers (Navaho Indians), 1:291, **3:263–265**, 3:264  
 Wise, John (military use of balloons), 1:92  
 Witt, James L. (FEMA director), 2:16  
 Women  
   cryptography opportunities (WW II), 1:131, 1:137  
   spies in the Civil War (U.S.), 1:211  
   Women Accepted for Voluntary Service Corps (WAVES), 1:137  
 Woodward, Bob, 1:202  
 Woodward, Gilbert, 2:458  
 Woolsey, R. James, 1:196, 1:311  
 World Bank, 2:99  
 World Health Organization (WHO), 1:249, 3:85, **3:265–266**  
 World Islamic Front for Jihad  
   Al-Qaeda and the Egyptian Islamic Jihad, 1:26  
 World Trade Center, 3:14, 3:69  
   history and construction, 3:268–269  
   9/11 aftermath and heroism, 3:269–270  
   9/11 attack, 1:26, 1:34–36, 1:196, 3:268–270  
   1993 bombing, 1:23, 1:134, 1:276, **3:266–268**, 3:267  
   tower collapse study, 1:50, 1:245  
   *See also* September 11 terrorist attacks  
 World War I, **3:270–274**  
   Black Tom explosion, 1:128–130  
   chemical warfare in, 1:180–181  
   costs of, 3:170  
   federal investigators in, 2:6  
   French protection of the Louvre's collection, 1:46  
   German code books captured by British, **3:274–275**  
   German cryptography, 1:3–4  
   German intelligence agency, 1:2  
   Treaty of Versailles, 2:226  
 World War II, **3:275–282**  
   Allies victories, 3:280–281  
   Axis victories, 3:278–279  
   CIA monitored broadcasts, 1:199  
   Combined Chiefs of Staff (U.S.—Britain), 2:190  
   Commissar Order (Germany), 1:3  
   FBI involvement in, 2:7  
   French protection of the Louvre's collection, 1:47  
   French resistance shuttling Allied servicemen, 2:43  
   Italian Army surrender, **3:283–284**  
   Operation Mincemeat and Sicily invasion, **3:282–283**  
   Pearl Harbor attack, 2:410–413  
   Radio Tokyo and Tokyo Rose, 3:163–164  
   reconnaissance aircraft, 1:75



U.K.-U.S. agreements to share information, 3:106–107  
World Wide Web, 1:171–172  
World Wide Web browsers, 2:142  
Wrath of God, 1:61–62, 2:283–284  
Wright, Orville, 2:298  
Wright, Peter, 1:404  
Wylér, Valeriano (Cuban leader), 3:101

## | X |

X-15 aircraft, 2:90–91  
X-ray fluorescence, 3:108  
X-ray machines  
  backscatter imaging, 3:53  
  CT scanners, 3:52  
  as detection devices, 1:135  
  used in passenger screening process, 1:22

projection radiography scanning, 3:51–52  
stereoscopic x-ray screening, 3:53  
technology refined, 1:175  
X-ray photoelectron spectroscopy, 3:108  
X-rays, medical and security uses, 1:383

## | Y |

Yale, Jr., Linus, 2:236  
Yamasaki, Minoru, 3:268  
Yardley, Herbert Osborne (ologist), 1:128  
Yeager, Charles E. “Chuck,” 2:90  
Yelsimov, Alexi, 3:75  
Yeltsin, Pres. Boris (Russian), 1:148, 1:172–173, 1:241  
Yersin, Alexandre, 1:144  
*Yersinia pestis*. *See* Bubonic plague  
Yom Kippur war, 2:284

Yoshikawa, Takeo, 2:412  
Young Hegelians, 3:148  
Yousef, Ramzi, 1:276  
Yucca Mountain, Nevada, 3:6–7  
Yugoslavia, Federal Republic, 1:138  
  Croatia and, 1:284

## | Z |

Zaire. *See* Congo  
Zapp, Walter, 1:158–159, 2:267  
Zeppelin, Ferdinand von, 1:93  
Zimmermann, Arthur, 1:290  
Zimmermann, Philip R., 1:291, 2:446  
Zinn, Herbert, 1:256  
Zinoviev, Grigory, 1:346  
Zinoviev letter forgery, 1:346  
Zoonoses, 3:286–287